IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

	§	
TAASERA LICENSING LLC,	§	Case No.
	§	
Plaintiff,	§	**JURY TRIAL DEMANDED**
	§	
v.	§	
	§	
FORTINET INC.,	§	
	§	
Defendant.	§	
	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Taasera Licensing LLC ("Taasera Licensing" or "Plaintiff") for its Complaint against Defendant Fortinet Inc. ("Fortinet" or "Defendant") alleges as follows:

THE PARTIES

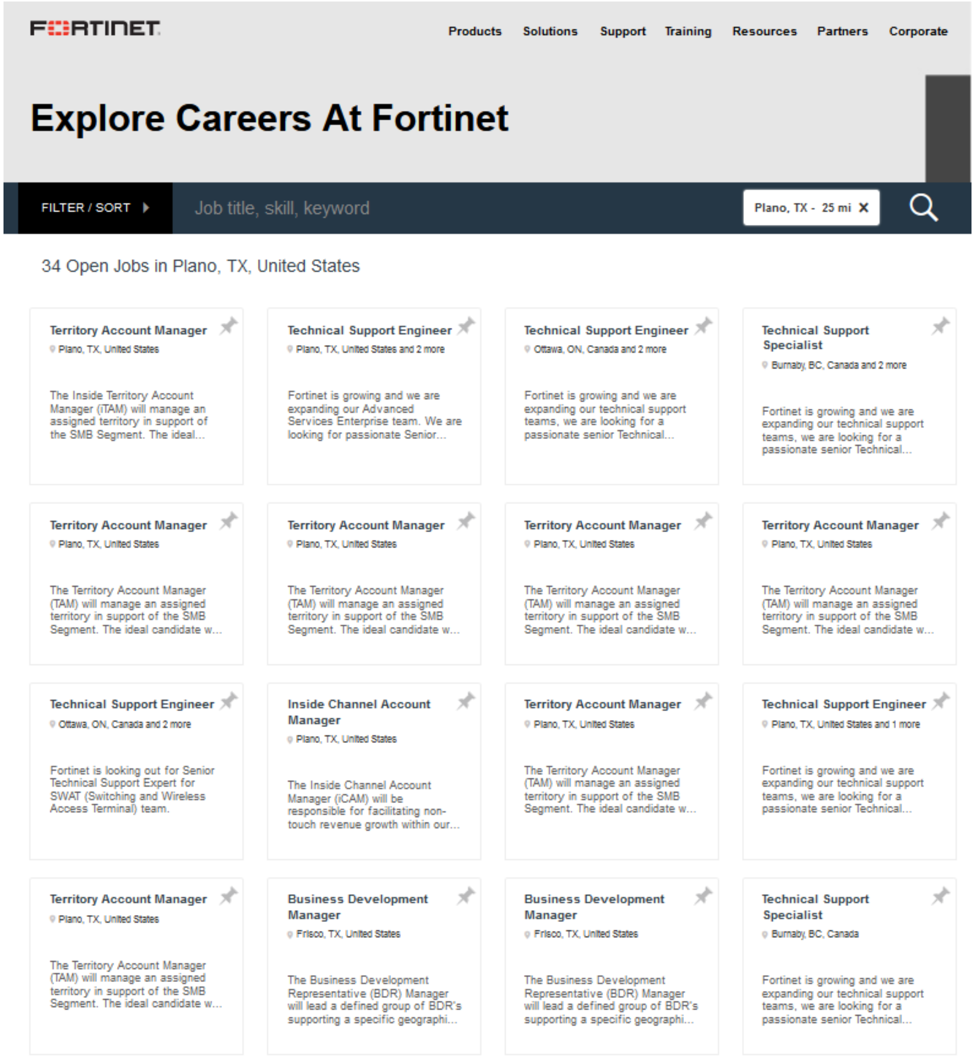
1. Taasera Licensing is a limited liability company organized and existing under the laws of the State of Texas, with its principal place of business located in Plano, Texas.

2. Upon information and belief, Defendant Fortinet Inc. is a corporation organized under the laws of the state of Delaware with a regular and established place of business in this Judicial District at 6111 W. Plano Parkway, #2100, Plano, Texas 75093. Upon information and belief, Fortinet does business in Texas and in the Eastern District of Texas, directly or through intermediaries. Defendant is registered to do business in the State of Texas and has been since at least November 24, 2009.

JURISDICTION

3. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over Fortinet. On information and belief, Fortinet conducts business and has committed acts of patent infringement and/or has induced and is currently inducing acts of patent infringement by others in this Judicial District and/or has contributed and is currently contributing to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States. Defendant currently lists 23 open positions in Plano, TX and Frisco, TX.



Explore Careers At Fortinet

34 Open Jobs in Plano, TX, United States

Territory Account Manager
Plano, TX, United States
The Inside Territory Account Manager (iTAM) will manage an assigned territory in support of the SMB Segment. The ideal...

Technical Support Engineer
Plano, TX, United States and 2 more
Fortinet is growing and we are expanding our Advanced Services Enterprise team. We are looking for passionate Senior...

Technical Support Engineer
Ottawa, ON, Canada and 2 more
Fortinet is growing and we are expanding our technical support teams, we are looking for a passionate senior Technical...

Technical Support Specialist
Burnaby, BC, Canada and 2 more
Fortinet is growing and we are expanding our technical support teams, we are looking for a passionate senior Technical...

Territory Account Manager
Plano, TX, United States
The Territory Account Manager (TAM) will manage an assigned territory in support of the SMB Segment. The ideal candidate w...

Territory Account Manager
Plano, TX, United States
The Territory Account Manager (TAM) will manage an assigned territory in support of the SMB Segment. The ideal candidate w...

Territory Account Manager
Plano, TX, United States
The Territory Account Manager (TAM) will manage an assigned territory in support of the SMB Segment. The ideal candidate w...

Territory Account Manager
Plano, TX, United States
The Territory Account Manager (TAM) will manage an assigned territory in support of the SMB Segment. The ideal candidate w...

Technical Support Engineer
Ottawa, ON, Canada and 2 more
Fortinet is looking out for Senior Technical Support Expert for SWAT (Switching and Wireless Access Terminal) team.

Inside Channel Account Manager
Plano, TX, United States
The Inside Channel Account Manager (iCAM) will be responsible for facilitating non-touch revenue growth within our...

Territory Account Manager
Plano, TX, United States
The Territory Account Manager (TAM) will manage an assigned territory in support of the SMB Segment. The ideal candidate w...

Technical Support Engineer
Plano, TX, United States and 1 more
Fortinet is growing and we are expanding our technical support teams, we are looking for a passionate senior Technical...

Territory Account Manager
Plano, TX, United States
The Territory Account Manager (TAM) will manage an assigned territory in support of the SMB Segment. The ideal candidate w...

Business Development Manager
Frisco, TX, United States
The Business Development Representative (BDR) Manager will lead a defined group of BDR's supporting a specific geographi...

Business Development Manager
Frisco, TX, United States
The Business Development Representative (BDR) Manager will lead a defined group of BDR's supporting a specific geographi...

Technical Support Specialist
Burnaby, BC, Canada
Fortinet is growing and we are expanding our technical support teams, we are looking for a passionate senior Technical...

[1]

5. Venue is proper in this Judicial District pursuant to 28 U.S.C. §§ 1391 and 1400(b). Fortinet has a regular and established place of business in this Judicial District, including in Collin County, and is deemed to reside in this Judicial District. On information and belief, Fortinet has committed acts of infringement in this Judicial District, and/or has purposely transacted business involving the Accused Products in this Judicial District including providing sales and technical support for the products accused of infringement herein. Upon information and belief, Fortinet

[1] https://edel.fa.us2.oraclecloud.com/hcmUI/CandidateExperience/en/sites/CX/requisitions?location=Plano%2C+TX%2C+United+States&locationId=300000003078988&locationLevel=city&mode=location&radius=25&radiusUnit=MI

directly or indirectly participated and currently participates in the stream of commerce that results in products, including the Accused Products, being made, used, tested, offered for sale, imported, and/or sold in the State of Texas and/or imported into the United States to the State of Texas, including this District.

6. On information and belief, Fortinet has hundreds of employees in this District—including executives, senior and mid-level officials, managerial staff, and first level positions in engineering, sales, marketing, customer service, and finance.

7. On information and belief, Fortinet's employees located in this District may have relevant information, including, in particular, information concerning the products and services Defendant provides, including the Accused Products, and how those products operate.

8. Fortinet's operations in this District include client outreach and sales for each of the Accused Products. As detailed above, Fortinet has customer-facing personnel and operations in this District. Fortinet also provides technical support to partners and customers for its products in this District.

9. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

10. On December 4, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,327,441 (the "'441 Patent") entitled "System and Method for Application Attestation." A true and correct copy of the '441 Patent is attached hereto as Exhibit A.

11. On August 26, 2014, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,819,419 (the "'419 Patent") entitled "Method and system for dynamic encryption of a URL." A true and correct copy of the '419 Patent is attached hereto as Exhibit B.

12. On February 10, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,955,038 (the "'038 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '038 Patent is attached hereto as Exhibit C.

13. On March 24, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,990,948 (the "'948 Patent") entitled "Systems and Methods for Orchestrating Runtime Operational Integrity." A true and correct copy of the '948 Patent is attached hereto as Exhibit D.

14. On July 28, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,092,616 (the "'616 Patent") entitled "Systems and Methods for Threat Identification and Remediation." A true and correct copy of the '616 Patent is attached hereto as Exhibit E.

15. On August 25, 2015, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,118,634 (the "'634 Patent") entitled "Dynamic encryption of a

universal resource locator." A true and correct copy of the '634 Patent is attached hereto as Exhibit F.

16. On March 28, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,608,997 (the "'997 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '997 Patent is attached hereto as Exhibit G.

17. On April 18, 2017, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,628,453 (the "'453 Patent") entitled "Dynamic encryption of a universal resource locator." A true and correct copy of the '453 Patent is available at A true and correct copy of the '453 Patent is attached hereto as Exhibit H.

18. On January 2, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,860,251 (the "'251 Patent") entitled "Dynamic encryption of a universal resource locator." A true and correct copy of the '251 Patent is available at A true and correct copy of the '251 Patent is attached hereto as Exhibit I.

19. On March 20, 2018, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 9,923,918 (the "'918 Patent") entitled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." A true and correct copy of the '918 Patent is attached hereto as Exhibit J.

20. Taasera Licensing is the sole and exclusive owner of all right, title, and interest in the '441 Patent, the '419 Patent, the '038 Patent, the '948 Patent, the '616 Patent, the '634 Patent, the '997 Patent, the '453 Patent, the '251 Patent, and the '918 Patent (collectively, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. Taasera Licensing also has

the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

FACTUAL ALLEGATIONS

21. The Patents-in-Suit generally cover systems and methods for network security systems.

22. Seven of the Patents-in-Suit were invented by International Business Machines ("IBM"). IBM pioneered the field of network security. Every year, IBM spends billions of dollars on research and development to invent, market, and sell new technology, and IBM obtains patents on many of the novel inventions that come out of that work, including the Patents-in-Suit. The seven patents invented by IBM are the result of the work from four different researchers, spanning over a decade.

23. Three of the Patents-in-Suit were developed by TaaSera, Inc. TaaSera, Inc. was a leader in preemptive breach detection systems, and comprised of security architects and subject matter experts with decades of experience in firewalls, intrusion detection, security event management, malware analysis, and endpoint security. The TaaSera, Inc. patents identify patterns of malicious coordinated network and endpoint behaviors.

24. The '441 Patent generally relates to technology for application attestation. The technology described in the '441 Patent was developed by Srinivas Kumar and Gurudatt Shashikumar of TaaSera, Inc.

25. The '419 Patent generally relates to technology hides web server file structure and protects unauthorized access to the web server by providing dynamic URL encryption. The technology described in the '419 Patent was developed by Michael P. Carlson and Srinivas Chowdhury of IBM.

26. The ’038 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the ’038 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

27. The ’948 Patent generally relates to technology that provides runtime operational integrity profiles identifying a threat level of subjects or applications. The technology described in the ’948 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

28. The ’616 Patent generally relates to technology that provides integrity profiles identifying a threat level of a system. The technology described in the ’616 Patent was developed by Srinivas Kumar and Dennis Pollutro of TaaSera, Inc.

29. The ’634 Patent generally relates to technology that hides web server file structure and protects unauthorized access to the web server by providing dynamic URL encryption. The technology described in the ’634 Patent was developed by Michael P. Carlson and Srinivas Chowdhury of IBM.

30. The ’997 Patent generally relates to technology that acts based on known security vulnerabilities to ensure endpoint compliance. The technology described in the ’997 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

31. The ’453 Patent generally relates to technology that hides web server file structure and protects unauthorized access to the web server by providing dynamic URL encryption. The technology described in the ’453 Patent was developed by Michael P. Carlson and Srinivas Chowdhury of IBM.

32. The ’251 Patent generally relates to technology that hides web server file structure and protects unauthorized access to the web server by providing dynamic URL encryption. The

technology described in the ’251 Patent was developed by Michael P. Carlson and Srinivas Chowdhury of IBM.

33. The ’918 Patent generally relates to technology that controls access to computing resources based on known security vulnerabilities. The technology described in the ’918 Patent was developed by Blair Nicodemus and Billy Edison Stephens of IBM.

34. Defendant has infringed and continues to infringe one or more of the Patents-in-Suit by making, using, testing, selling, offering to sell, and/or importing, and by actively inducing others to make, use, sell, offer to sell, and/or import products that implement the network security inventions claimed in the Patents-in Suit. For example, the Accused Products include at least Fortinet FortiEDR and Fortiweb.

35. TaaSera, Inc. manufactured commercial and academic versions of its NetTrust Security Appliance. NetTrust combined breach detection with security analytics to identify hidden threatening network behaviors. The analytics engine analyzed behavioral profiles, threat patterns, and contextual evidence to rank systems by their risk of breach.

36. Upon information and belief, Taasera Licensing and its predecessors have complied with the requirements of 35 U.S.C. § 287(a).

COUNT I
(Infringement of the ’441 Patent)

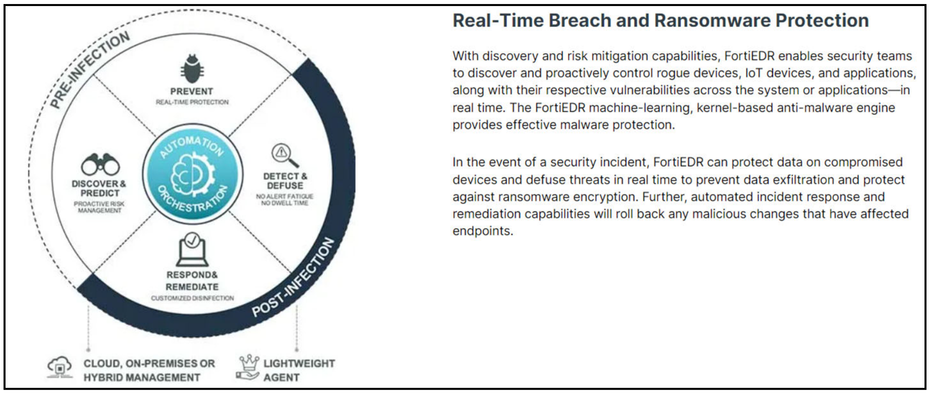
37. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

38. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’441 Patent.

39. Defendant has and continues to directly infringe at least claim 1 of the ’441 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States

products that satisfy each and every limitation of one or more claims of the ’441 Patent. Such products incorporate the Real-Time Breach and Ransomware Protection feature and include at least the Fortinet FortiEDR (the “’441 Accused Products”) which practice a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server, comprising: receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application; and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components; generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result; and sending, by the attestation server, the attestation result associated with the application.

40. Every ’441 Accused Product practices a method of providing an attestation service for an application at runtime executing on a computing platform using an attestation server. For example, Fortinet FortiEDR incorporates Real-Time Breach and Ransomware Protection to discover and proactively control rogue applications.



Real-Time Breach and Ransomware Protection

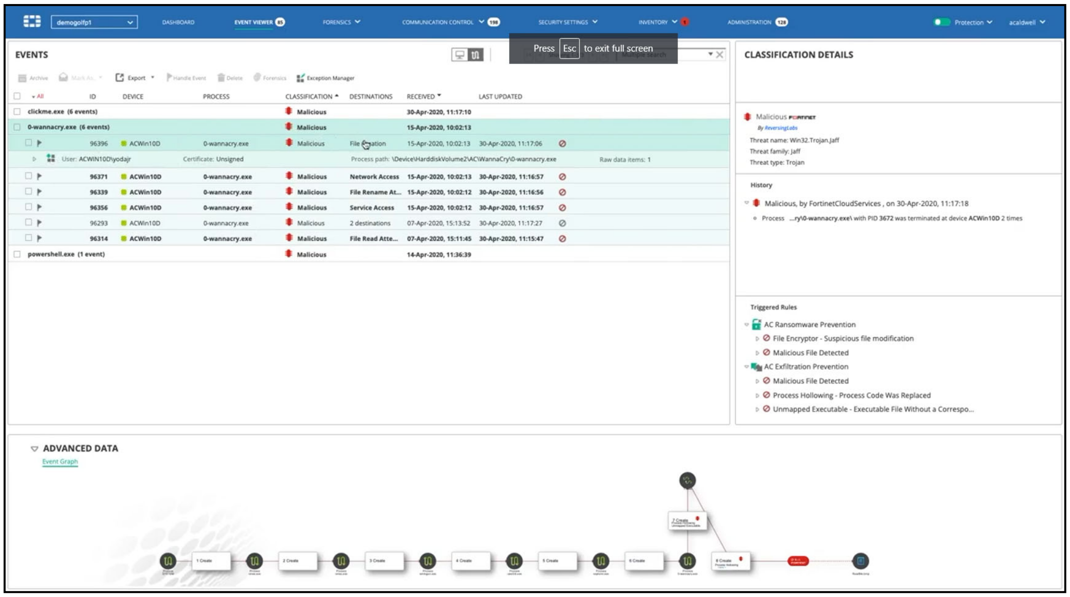
With discovery and risk mitigation capabilities, FortiEDR enables security teams to discover and proactively control rogue devices, IoT devices, and applications, along with their respective vulnerabilities across the system or applications—in real time. The FortiEDR machine-learning, kernel-based anti-malware engine provides effective malware protection.

In the event of a security incident, FortiEDR can protect data on compromised devices and defuse threats in real time to prevent data exfiltration and protect against ransomware encryption. Further, automated incident response and remediation capabilities will roll back any malicious changes that have affected endpoints.

[2]

41. Every ’441 Accused Product practices receiving, by the attestation server remote from the computing platform: a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application, and a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components. For example, Fortinet FortiEDR receives process attributes, context information, and processes behavior information for detected threats.

[2] https://www.fortinet.com/products/endpoint-security/fortiedr



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
	User: ACWIN10D\yodajr		Certificate: Unsigned		Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe		Raw data items: 1
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

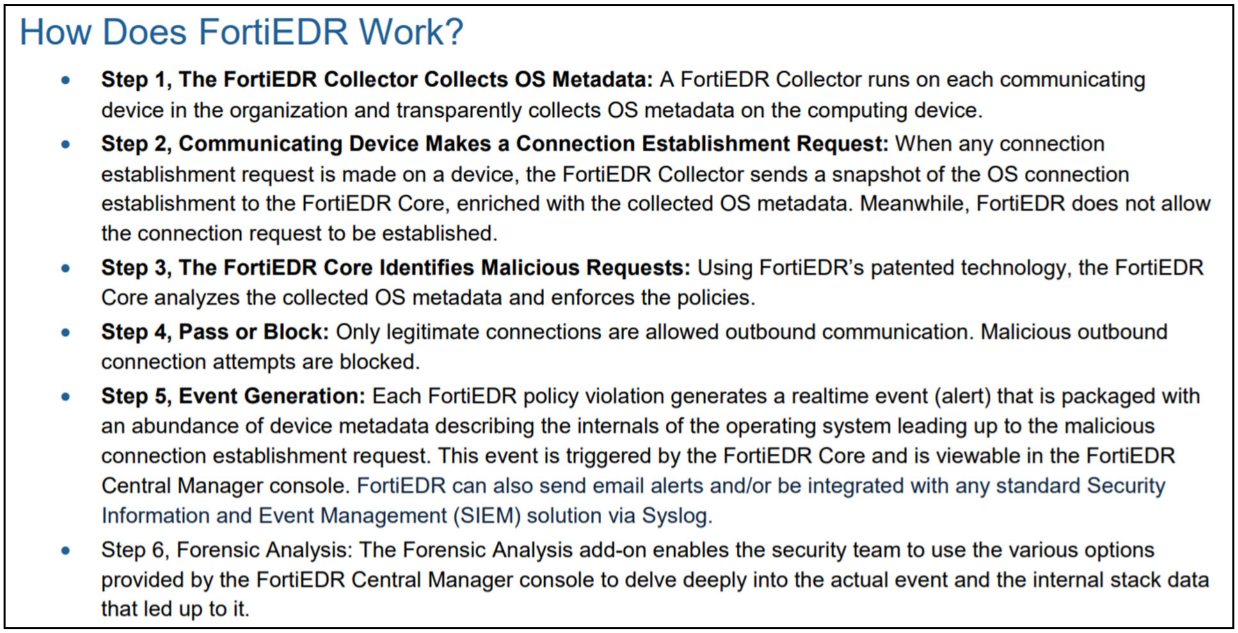
Triggered Rules

- AC Ransomware Prevention
  - File Encryptor - Suspicious file modification
  - Malicious File Detected
- AC Exfiltration Prevention
  - Malicious File Detected
  - Process Hollowing - Process Code Was Replaced
  - Unmapped Executable - Executable File Without a Correspo...

[3]

42. Every ’441 Accused Product practices generating, by the attestation server, a report indicating security risks associated with the application based on the received runtime execution context and the received security context, as an attestation result and sending, by the attestation server, the attestation result associated with the application. For example, Fortinet FortiEDR sends alerts and logs information related to each detected threat, including the result of the detected threat.[4]

[3] https://www.youtube.com/watch?v=_DoSSI9fPAk
[4] *Id*.



How Does FortiEDR Work?

- **Step 1, The FortiEDR Collector Collects OS Metadata:** A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
- **Step 2, Communicating Device Makes a Connection Establishment Request:** When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established.
- **Step 3, The FortiEDR Core Identifies Malicious Requests:** Using FortiEDR's patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies.
- **Step 4, Pass or Block:** Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked.
- **Step 5, Event Generation:** Each FortiEDR policy violation generates a realtime event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog.
- Step 6, Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual event and the internal stack data that led up to it.

[5]

43. Defendant has and continues to indirectly infringe one or more claims of the '441 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as '441 Accused Products (*e.g.*, products incorporating the Real-Time Breach and Ransomware Protection feature).

44. Defendant, with knowledge that these products, or the use thereof, infringe the '441 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '441 Patent by providing these products to others, including customers and end-users, for use in an infringing manner, as well as

[5] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf

providing demonstrations, training, instruction courses, instruction manuals, installation manuals, and customer service that instruct end-users to use the products in an infringing manner.[6]

45. Defendant encourages and induces its users and customers of the '441 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[7]

46. Defendant further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging FortiEDR Collector software to be installed on individual endpoint computers.[8]

47. Defendant induced and is currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '441 Patent, but while remaining willfully blind to the infringement.

48. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '441 Patent in an amount to be proved at trial.

49. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '441 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

[6] https://www.fortinet.com/products/endpoint-security/fortiedr/demo; https://training.fortinet.com/local/staticpage/view.php?page=library_fortiedr; https://training.fortinet.com/; https://www.fortinet.com/products/endpoint-security/fortiedr; https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

[7] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[8] https://docs.fortinet.com/document/fortiedr/5.1.0/administration-guide/186029/installing-fortiedr-collectors

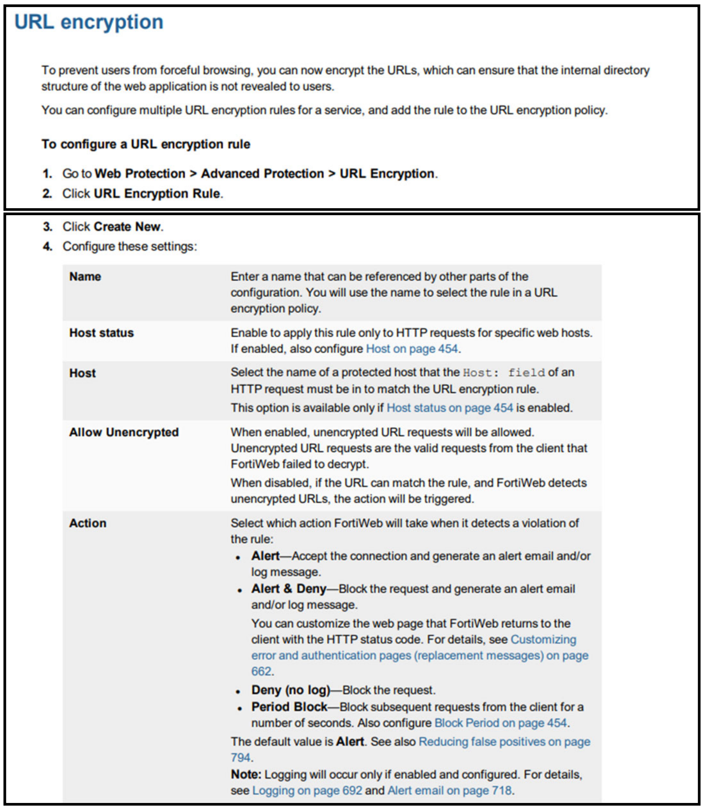
COUNT II
(Infringement of the ’419 Patent)

50. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

51. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’419 Patent.

52. Defendant has and continues to directly infringe at least claim 13 of the ’419 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’419 Patent. Such products incorporate the URL Encryption feature and include at least Fortinet Fortiweb (the “’419 Accused Products”) which is a computer program product stored in a computer readable hardware storage device for restricting access to information transmitted over a computing network, said computer program product comprising: instructions for receiving at a network location a resource request for a resource to be located, said resource request containing a universal resource locator (URL); instructions for evaluating the URL to determine whether encryption of the URL is required; instructions for locating the requested resource contained in the resource request, when encryption of the URL is not required; instructions for determining whether the requested resource is available; and instructions for determining whether encryption of a return URL of the requested resource is required, when the requested resource is available.

53. Every ’419 Accused Product is a computer program product stored in a computer readable hardware storage device for restricting access to information transmitted over a computing network. For example, the Fortinet Fortiweb performs URL encryption.



URL encryption

To prevent users from forceful browsing, you can now encrypt the URLs, which can ensure that the internal directory structure of the web application is not revealed to users.

You can configure multiple URL encryption rules for a service, and add the rule to the URL encryption policy.

To configure a URL encryption rule

1. Go to **Web Protection > Advanced Protection > URL Encryption**.
2. Click **URL Encryption Rule**.
3. Click **Create New**.
4. Configure these settings:

Name	Enter a name that can be referenced by other parts of the configuration. You will use the name to select the rule in a URL encryption policy.
Host status	Enable to apply this rule only to HTTP requests for specific web hosts. If enabled, also configure Host on page 454.
Host	Select the name of a protected host that the `Host: field` of an HTTP request must be in to match the URL encryption rule. This option is available only if Host status on page 454 is enabled.
Allow Unencrypted	When enabled, unencrypted URL requests will be allowed. Unencrypted URL requests are the valid requests from the client that FortiWeb failed to decrypt. When disabled, if the URL can match the rule, and FortiWeb detects unencrypted URLs, the action will be triggered.
Action	Select which action FortiWeb will take when it detects a violation of the rule: • **Alert**—Accept the connection and generate an alert email and/or log message. • **Alert & Deny**—Block the request and generate an alert email and/or log message. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see Customizing error and authentication pages (replacement messages) on page 662. • **Deny (no log)**—Block the request. • **Period Block**—Block subsequent requests from the client for a number of seconds. Also configure Block Period on page 454. The default value is **Alert**. See also Reducing false positives on page 794. **Note:** Logging will occur only if enabled and configured. For details, see Logging on page 692 and Alert email on page 718.

[9]

54. Every ’419 Accused Product contains instructions for receiving at a network location a resource request for a resource to be located, said resource request containing a universal resource locator (URL). For example, Fortinet Fortiweb receives request URLs for resources to be located.[10]

55. Every ’419 Accused Product contains instructions for evaluating the URL to determine whether encryption of the URL is required. For example, Fortinet Fortiweb evaluates whether the URL is listed as a request URL or in an exception list.[11]

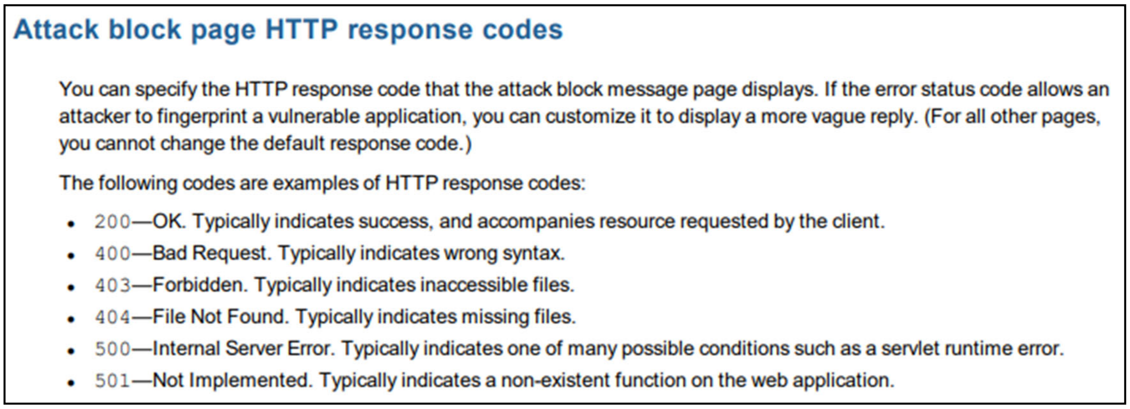
56. Every ’419 Accused Product contains instructions for locating the requested resource contained in the resource request, when encryption of the URL is not required and

[9] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/5a6875be-586e-11ea-9384-00505692583a/FortiWeb_6.3.1_Administration_Guide.pdf

[10] *Id.*

[11] *Id.*

instructions for determining whether the requested resource is available. For example, if Fortinet Fortiweb is not able to locate the file, it will return a 404 (file not found) error code.



Attack block page HTTP response codes

You can specify the HTTP response code that the attack block message page displays. If the error status code allows an attacker to fingerprint a vulnerable application, you can customize it to display a more vague reply. (For all other pages, you cannot change the default response code.)

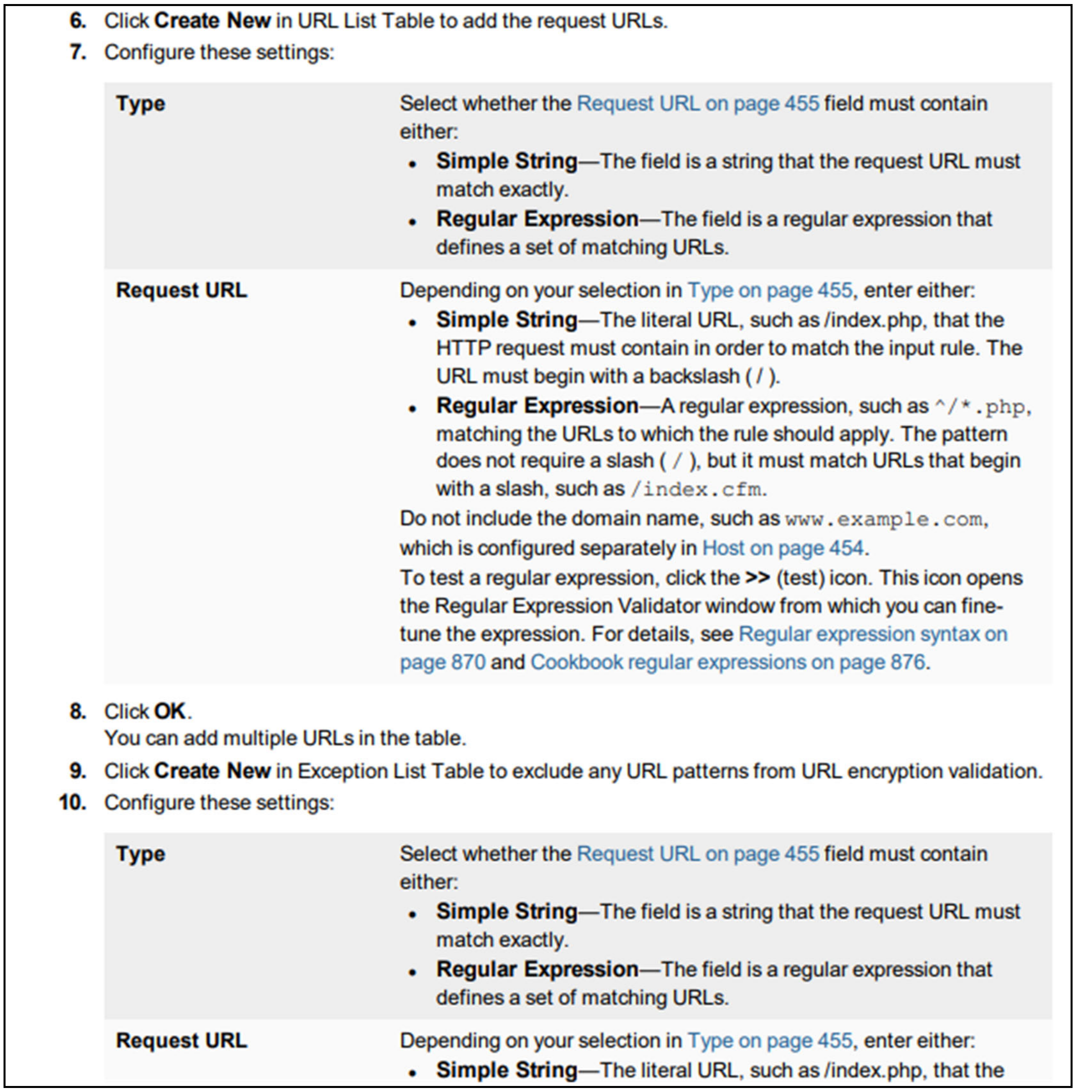
The following codes are examples of HTTP response codes:

- `200`—OK. Typically indicates success, and accompanies resource requested by the client.
- `400`—Bad Request. Typically indicates wrong syntax.
- `403`—Forbidden. Typically indicates inaccessible files.
- `404`—File Not Found. Typically indicates missing files.
- `500`—Internal Server Error. Typically indicates one of many possible conditions such as a servlet runtime error.
- `501`—Not Implemented. Typically indicates a non-existent function on the web application.

[12]

57. Every ’419 Accused Product contains instructions for determining whether encryption of a return URL of the requested resource is required, when the requested resource is available. For example, Fortinet Fortiweb encrypts all request URLs.

[12] *Id.*



6. Click **Create New** in URL List Table to add the request URLs.
7. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (/). • **Regular Expression**—A regular expression, such as `^/*.php`, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as `/index.cfm`. Do not include the domain name, such as `www.example.com`, which is configured separately in Host on page 454. To test a regular expression, click the **>>** (test) icon. This icon opens the Regular Expression Validator window from which you can fine-tune the expression. For details, see Regular expression syntax on page 870 and Cookbook regular expressions on page 876.

8. Click **OK**.
   You can add multiple URLs in the table.
9. Click **Create New** in Exception List Table to exclude any URL patterns from URL encryption validation.
10. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the

[13]

58. Defendant has and continues to indirectly infringe one or more claims of the ’419 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as ’419 Accused Products (*e.g.*, products incorporating the URL Encryption feature).

[13] *Id*.

59. Defendant, with knowledge that these products, or the use thereof, infringe the '419 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '419 Patent by providing these products to others, including customers and end users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, deployment guides, and customer service that instruct customers to use the products in an infringing manner.[14]

60. Defendant encourages and induces its users and customers of the '419 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security products available on its website, widely advertises those products, provides applications that allow customers and users to access those products, provides training and instructions for deploying and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[15]

61. Defendant further encourages and induces its customers and users to use the infringing Fortiweb product by providing directions for deploying and using Fortiweb.[16]

62. Defendant induced and is currently inducing infringement by others, including customers and end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the '419 Patent, but while remaining willfully blind to the infringement.

63. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '419 Patent in an amount to be proved at trial.

[14] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0

[15] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[16] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0

64. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '419 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT III
(Infringement of the '038 Patent)

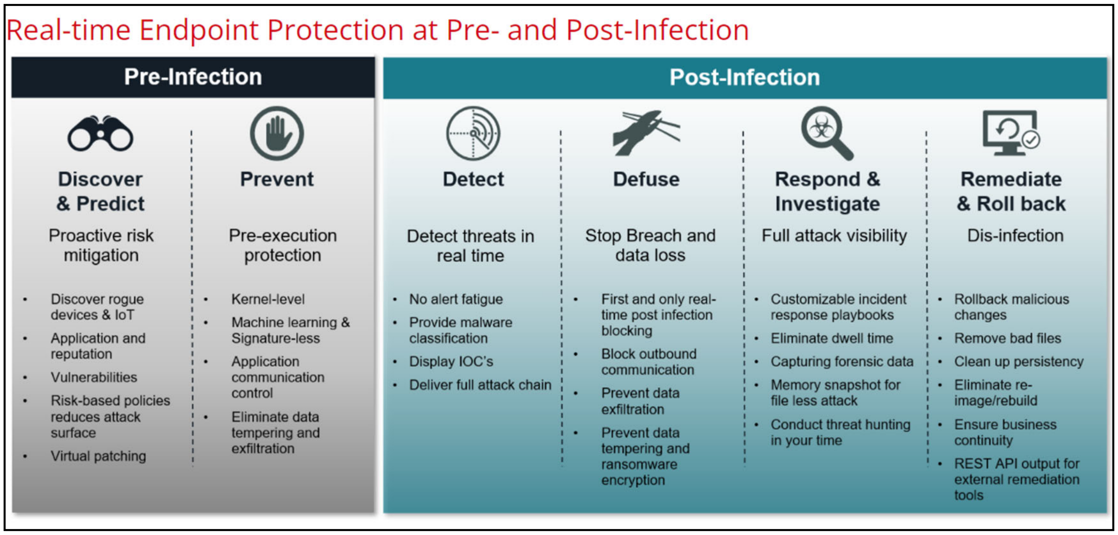
65. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

66. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '038 Patent.

67. Defendant has and continues to directly infringe at least claim 23 of the '038 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '038 Patent. Such products incorporate the threat classification and remediation features and include at least Fortinet FortiEDR (the "'038 Accused Products") which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and initiating, by the computing system, based on the compliance state,

an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

68. Every ’038 Accused Product practices a method for controlling the operation of an endpoint. For example, the Fortinet FortiEDR performs remediation on endpoints.



Real-time Endpoint Protection at Pre- and Post-Infection

Pre-Infection

Discover & Predict

Proactive risk mitigation

- Discover rogue devices & IoT
- Application and reputation
- Vulnerabilities
- Risk-based policies reduces attack surface
- Virtual patching

Prevent

Pre-execution protection

- Kernel-level
- Machine learning & Signature-less
- Application communication control
- Eliminate data tempering and exfiltration

Post-Infection

Detect

Detect threats in real time

- No alert fatigue
- Provide malware classification
- Display IOC’s
- Deliver full attack chain

Defuse

Stop Breach and data loss

- First and only real-time post infection blocking
- Block outbound communication
- Prevent data exfiltration
- Prevent data tempering and ransomware encryption

Respond & Investigate

Full attack visibility

- Customizable incident response playbooks
- Eliminate dwell time
- Capturing forensic data
- Memory snapshot for file less attack
- Conduct threat hunting in your time

Remediate & Roll back

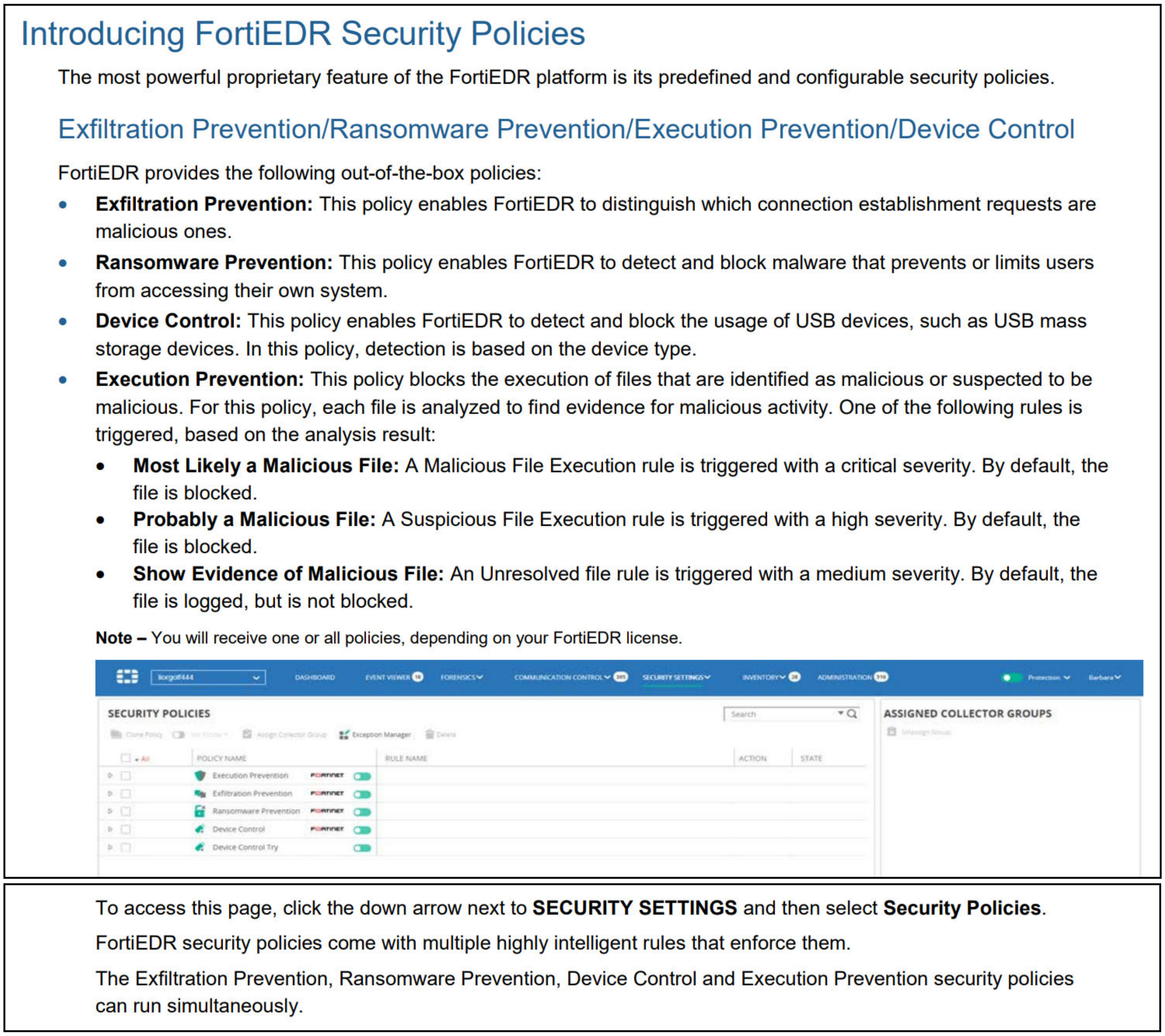
Dis-infection

- Rollback malicious changes
- Remove bad files
- Clean up persistency
- Eliminate re-image/rebuild
- Ensure business continuity
- REST API output for external remediation tools

[17]

69. Every ’038 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies and maintaining the plurality of policies in a data store on the computing system. For example, Fortinet FortiEDR allows configuration of a plurality of policies (*e.g.*, security policies) at a system remote from the endpoint through a provided user interface which are stored in a data store.

[17] https://www.avfirewalls.com/FortiEDR.asp



Introducing FortiEDR Security Policies

The most powerful proprietary feature of the FortiEDR platform is its predefined and configurable security policies.

Exfiltration Prevention/Ransomware Prevention/Execution Prevention/Device Control

FortiEDR provides the following out-of-the-box policies:

- **Exfiltration Prevention:** This policy enables FortiEDR to distinguish which connection establishment requests are malicious ones.
- **Ransomware Prevention:** This policy enables FortiEDR to detect and block malware that prevents or limits users from accessing their own system.
- **Device Control:** This policy enables FortiEDR to detect and block the usage of USB devices, such as USB mass storage devices. In this policy, detection is based on the device type.
- **Execution Prevention:** This policy blocks the execution of files that are identified as malicious or suspected to be malicious. For this policy, each file is analyzed to find evidence for malicious activity. One of the following rules is triggered, based on the analysis result:
  - **Most Likely a Malicious File:** A Malicious File Execution rule is triggered with a critical severity. By default, the file is blocked.
  - **Probably a Malicious File:** A Suspicious File Execution rule is triggered with a high severity. By default, the file is blocked.
  - **Show Evidence of Malicious File:** An Unresolved file rule is triggered with a medium severity. By default, the file is logged, but is not blocked.

Note – You will receive one or all policies, depending on your FortiEDR license.

All	POLICY NAME		RULE NAME	ACTION	STATE
	Execution Prevention	FORTINET			
	Exfiltration Prevention	FORTINET			
	Ransomware Prevention	FORTINET			
	Device Control	FORTINET			
	Device Control Try				

To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.

FortiEDR security policies come with multiple highly intelligent rules that enforce them.

The Exfiltration Prevention, Ransomware Prevention, Device Control and Execution Prevention security policies can run simultaneously.

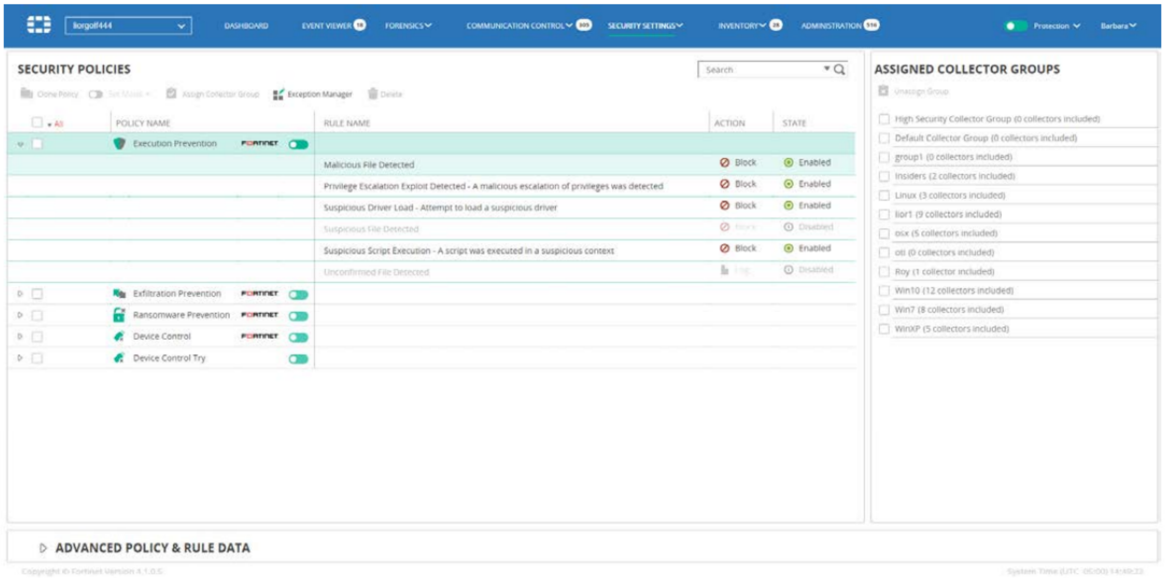
[18]

70. Every ’038 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, the Fortinet FortiEDR security policies identify, from the plurality of polices, operating conditions on the endpoint (such as the operating conditions listed in the “rules”) to monitor.

[18] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf

Security Policies Page

The **SECURITY POLICIES** page displays a row for each security policy. Each policy row can be expanded to show the rules that it contains, as shown below. To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.



POLICY NAME		RULE NAME	ACTION	STATE
Execution Prevention	FORTINET			
		Malicious File Detected	Block	Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
		Suspicious File Detected	Block	Disabled
		Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
		Unconfirmed File Detected	Log	Disabled
Exfiltration Prevention	FORTINET			
Ransomware Prevention	FORTINET			
Device Control	FORTINET			
Device Control Try				

□ High Security Collector Group (0 collectors included)
□ Default Collector Group (0 collectors included)
□ group1 (0 collectors included)
□ Insiders (2 collectors included)
□ Linux (3 collectors included)
□ lior1 (9 collectors included)
□ osx (5 collectors included)
□ oti (0 collectors included)
□ Roy (1 collector included)
□ Win10 (12 collectors included)
□ Win7 (8 collectors included)
□ WinXP (5 collectors included)

FortiEDR is provided out-of-the-box with several predefined security policies (depending on your license), ready for you to get started. By default, all policies are set to **Simulation** mode (meaning that they ***only*** log and ***do not block***) and show the FORTINET logo. This page also enables you to define additional policies.

Exfiltration prevention policies are marked with the icon, ransomware prevention policies are marked with the icon, execution prevention policies are marked with the icon and device control policies are marked with the icon.

The following information is defined per security policy:

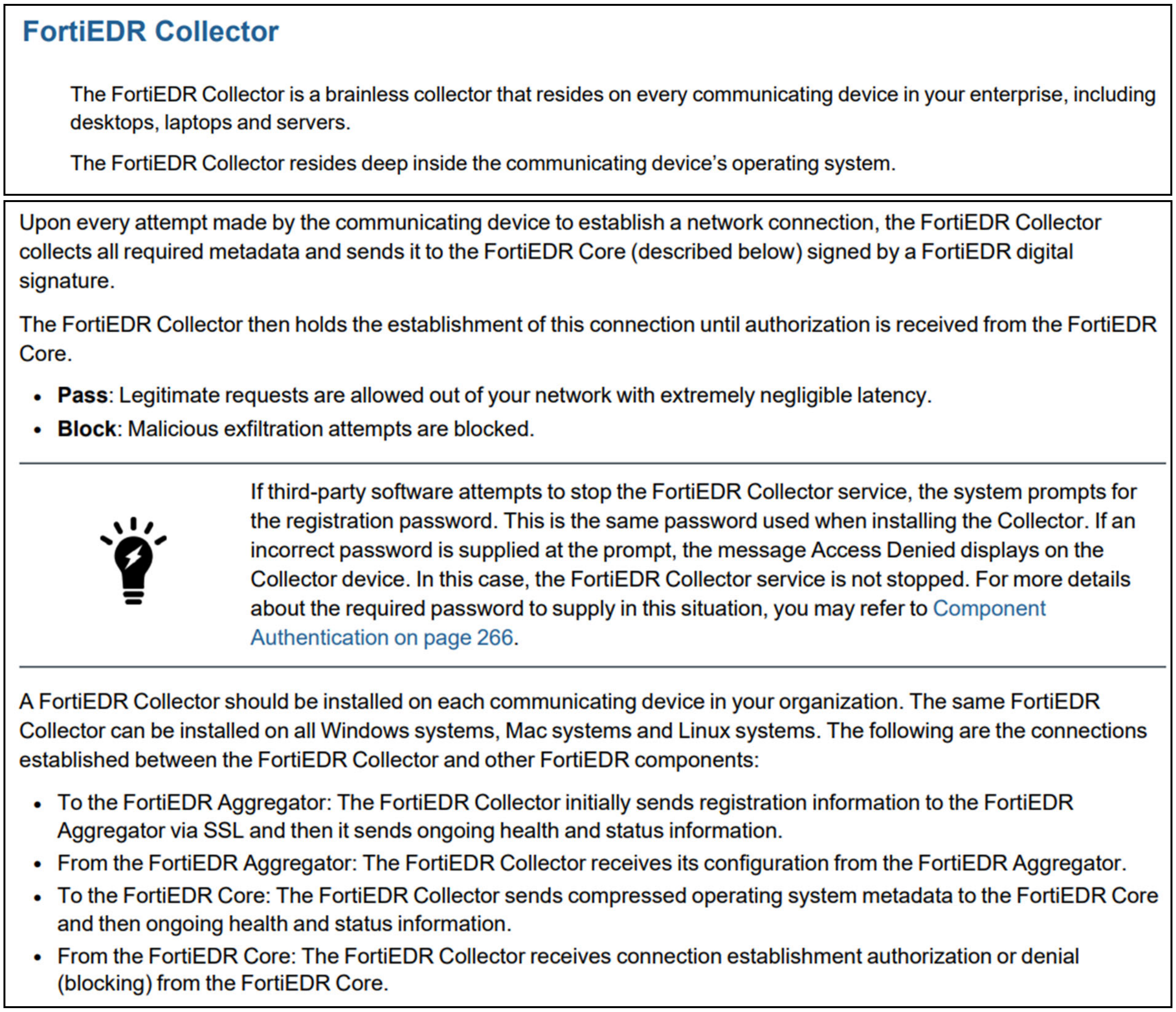
Note – Only the **ACTION** (described below) and the **STATE** (Enabled/Disabled) column of a rule can be changed by you.

- **POLICY NAME:** The policy name appears in the leftmost column. The policy name is defined when the policy is created. The name of the **Default Policy** cannot be changed.
- **RULE NAME:** FortiEDR's proprietary rules come predefined and are the primary component of FortiEDR's proprietary security solution. This column displays a short description for the purpose of this rule.

[19]

71. Every '038 Accused Product practices configuring one or more software agents on the endpoint to monitor the plurality of operating conditions. For example, Fortinet FortiEDR configures the FortiEDR Collectors to monitor the plurality of operating conditions (*e.g.*, operating system metadata).

[19] *Id*.



FortiEDR Collector

The FortiEDR Collector is a brainless collector that resides on every communicating device in your enterprise, including desktops, laptops and servers.

The FortiEDR Collector resides deep inside the communicating device's operating system.

Upon every attempt made by the communicating device to establish a network connection, the FortiEDR Collector collects all required metadata and sends it to the FortiEDR Core (described below) signed by a FortiEDR digital signature.

The FortiEDR Collector then holds the establishment of this connection until authorization is received from the FortiEDR Core.

- **Pass**: Legitimate requests are allowed out of your network with extremely negligible latency.
- **Block**: Malicious exfiltration attempts are blocked.

If third-party software attempts to stop the FortiEDR Collector service, the system prompts for the registration password. This is the same password used when installing the Collector. If an incorrect password is supplied at the prompt, the message Access Denied displays on the Collector device. In this case, the FortiEDR Collector service is not stopped. For more details about the required password to supply in this situation, you may refer to Component Authentication on page 266.

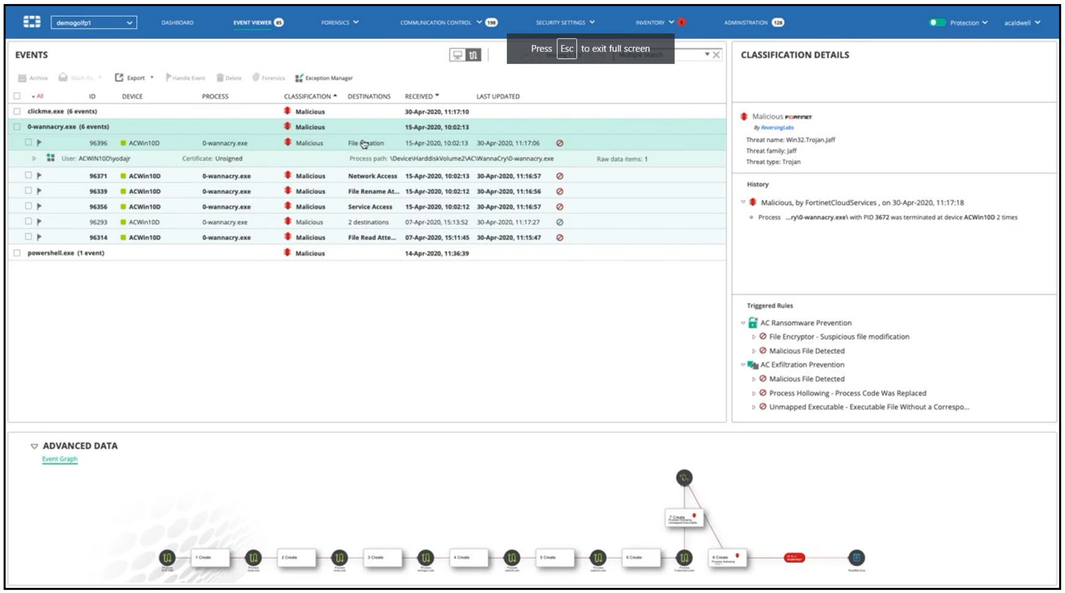
A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows systems, Mac systems and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- To the FortiEDR Aggregator: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health and status information.
- From the FortiEDR Aggregator: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.
- To the FortiEDR Core: The FortiEDR Collector sends compressed operating system metadata to the FortiEDR Core and then ongoing health and status information.
- From the FortiEDR Core: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

[20]

72. Every '038 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents. For example, FortiEDR receives events, gathered by the one or more software agents (*e.g.*, FortiEDR Collectors).[21]

[20] *Id.*
[21] *Id.*



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
User: ACWIN10D\yodajr			Certificate: Unsigned		Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe		Raw data items: 1
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

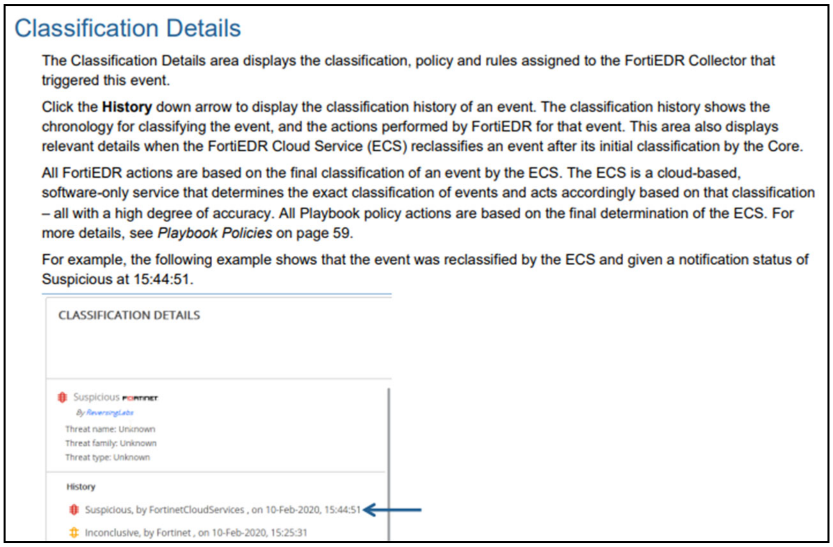
Triggered Rules

- AC Ransomware Prevention
  - File Encryptor - Suspicious file modification
  - Malicious File Detected
- AC Exfiltration Prevention
  - Malicious File Detected
  - Process Hollowing - Process Code Was Replaced
  - Unmapped Executable - Executable File Without a Correspo...

[22]

73. Every ’038 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information (*e.g.*, events) and a plurality of compliance policies in the data store. For example, Fortinet FortiEDR determines a compliance state (e.g., classifies events) of the endpoint based on the status information and the security policies. [23]

[22] https://www.youtube.com/watch?v=_DoSSI9fPAk
[23] *Id*.



Classification Details

The Classification Details area displays the classification, policy and rules assigned to the FortiEDR Collector that triggered this event.

Click the **History** down arrow to display the classification history of an event. The classification history shows the chronology for classifying the event, and the actions performed by FortiEDR for that event. This area also displays relevant details when the FortiEDR Cloud Service (ECS) reclassifies an event after its initial classification by the Core.

All FortiEDR actions are based on the final classification of an event by the ECS. The ECS is a cloud-based, software-only service that determines the exact classification of events and acts accordingly based on that classification – all with a high degree of accuracy. All Playbook policy actions are based on the final determination of the ECS. For more details, see *Playbook Policies* on page 59.

For example, the following example shows that the event was reclassified by the ECS and given a notification status of Suspicious at 15:44:51.

CLASSIFICATION DETAILS

Suspicious FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

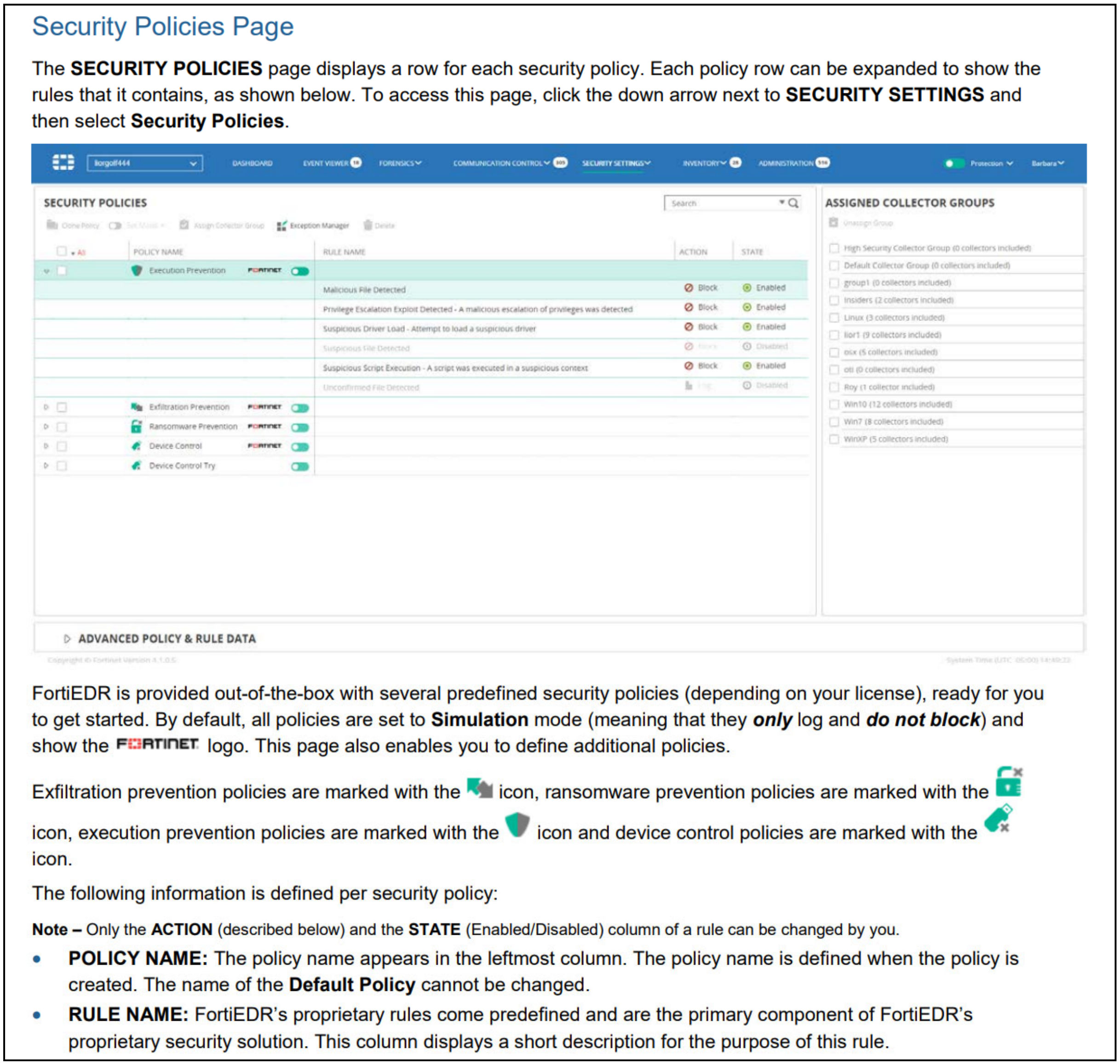
History

Suspicious, by FortinetCloudServices , on 10-Feb-2020, 15:44:51
Inconclusive, by Fortinet , on 10-Feb-2020, 15:25:31

[24]

74. Every ’038 Accused Product practices initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint. For example, Fortinet FortiEDR remediation initiates actions identified in the security policy rules based on the compliance state which are carried out by the endpoint processor.

[24] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf



Security Policies Page

The **SECURITY POLICIES** page displays a row for each security policy. Each policy row can be expanded to show the rules that it contains, as shown below. To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.

□ All	POLICY NAME		RULE NAME	ACTION	STATE
□	Execution Prevention	FORTINET			
			Malicious File Detected	Block	Enabled
			Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
			Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
			Suspicious File Detected	Block	Disabled
			Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
			Unconfirmed File Detected	Log	Disabled
□	Exfiltration Prevention	FORTINET			
□	Ransomware Prevention	FORTINET			
□	Device Control	FORTINET			
□	Device Control Try				

- □ High Security Collector Group (0 collectors included)
- □ Default Collector Group (0 collectors included)
- □ group1 (0 collectors included)
- □ Insiders (2 collectors included)
- □ Linux (3 collectors included)
- □ lior1 (9 collectors included)
- □ osx (5 collectors included)
- □ oti (0 collectors included)
- □ Roy (1 collector included)
- □ Win10 (12 collectors included)
- □ Win7 (8 collectors included)
- □ WinXP (5 collectors included)

FortiEDR is provided out-of-the-box with several predefined security policies (depending on your license), ready for you to get started. By default, all policies are set to **Simulation** mode (meaning that they ***only*** log and ***do not block***) and show the FORTINET logo. This page also enables you to define additional policies.

Exfiltration prevention policies are marked with the icon, ransomware prevention policies are marked with the icon, execution prevention policies are marked with the icon and device control policies are marked with the icon.

The following information is defined per security policy:

Note – Only the **ACTION** (described below) and the **STATE** (Enabled/Disabled) column of a rule can be changed by you.

- **POLICY NAME:** The policy name appears in the leftmost column. The policy name is defined when the policy is created. The name of the **Default Policy** cannot be changed.
- **RULE NAME:** FortiEDR's proprietary rules come predefined and are the primary component of FortiEDR's proprietary security solution. This column displays a short description for the purpose of this rule.

[25]

75. Defendant has and continues to indirectly infringe one or more claims of the ’038 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include

[25] *Id*.

infringing technology, such as ’038 Accused Products (*e.g.*, products incorporating the threat classification and remediation features).

76. Defendant, with knowledge that these products, or the use thereof, infringe the ’038 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’038 Patent by providing these products to others, including customers and end-users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, installation manuals, and customer service that instruct end-users to use the products in an infringing manner.[26]

77. Defendant encourages and induces its users and customers of the ’038 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[27]

78. Defendant further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging FortiEDR Collector software to be installed on individual endpoint computers.[28]

79. Defendant induced and is currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that

[26] https://www.fortinet.com/products/endpoint-security/fortiedr/demo; https://training.fortinet.com/local/staticpage/view.php?page=library_fortiedr; https://training.fortinet.com/; https://www.fortinet.com/products/endpoint-security/fortiedr; https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

[27] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[28] https://docs.fortinet.com/document/fortiedr/5.1.0/administration-guide/186029/installing-fortiedr-collectors

there was a high probability that others, including end-users, infringe the ’038 Patent, but while remaining willfully blind to the infringement.

80. Taasera Licensing has suffered damages as a result of Defendant’s direct and indirect infringement of the ’038 Patent in an amount to be proved at trial.

81. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’038 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT IV
(Infringement of the ’948 Patent)

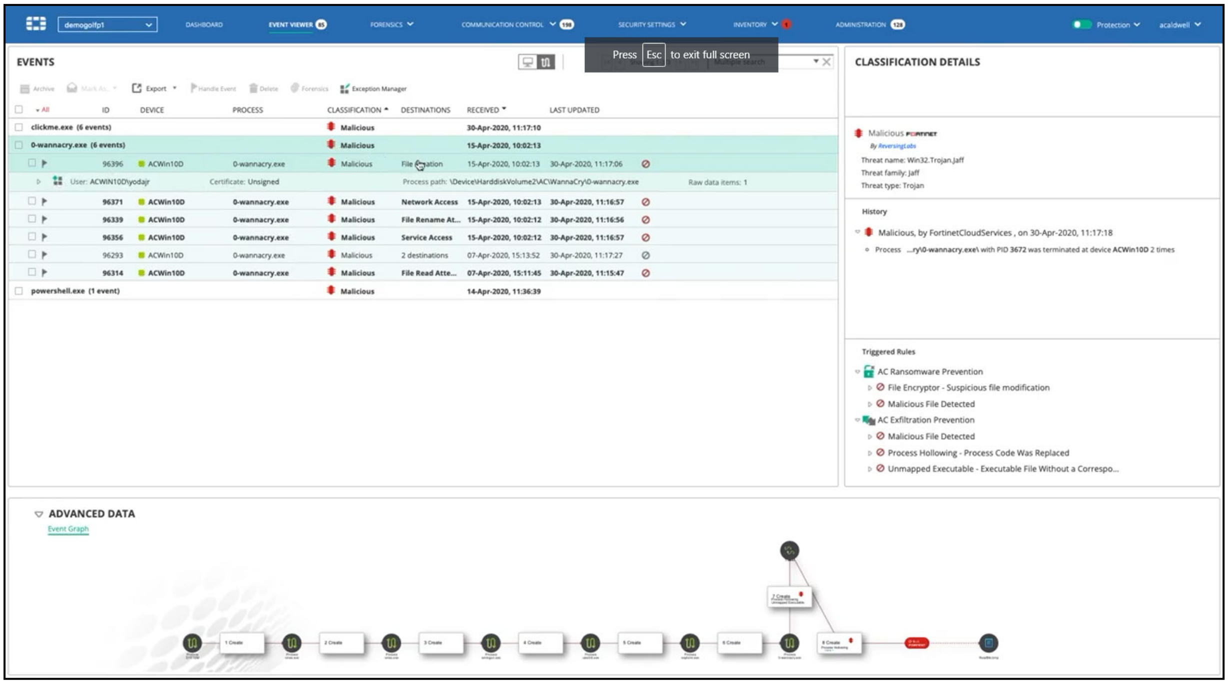
82. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

83. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’948 Patent.

84. Defendant has and continues to directly infringe at least claim 1 of the ’948 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’948 Patent. Such products incorporate the application behavioral analysis feature and include at least the Fortinet FortiEDR (the “’948 Accused Products”) which practice a method of providing real-time operational integrity of an application on a native computing environment, the method comprising: monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application; generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event

correlation matrix, a risk correlation matrix, and a trust supervisor; correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

85. Every ’948 Accused Product practices a method of providing real-time operational integrity of an application on a native computing environment. For example, the Fortinet FortiEDR incorporates application integrity monitoring and behavior analysis.



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
User: ACWIN10D\yodajr		Certificate: Unsigned			Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe		Raw data items: 1
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

Triggered Rules

- AC Ransomware Prevention
  - File Encryptor - Suspicious file modification
  - Malicious File Detected
- AC Exfiltration Prevention
  - Malicious File Detected
  - Process Hollowing - Process Code Was Replaced
  - Unmapped Executable - Executable File Without a Correspo...

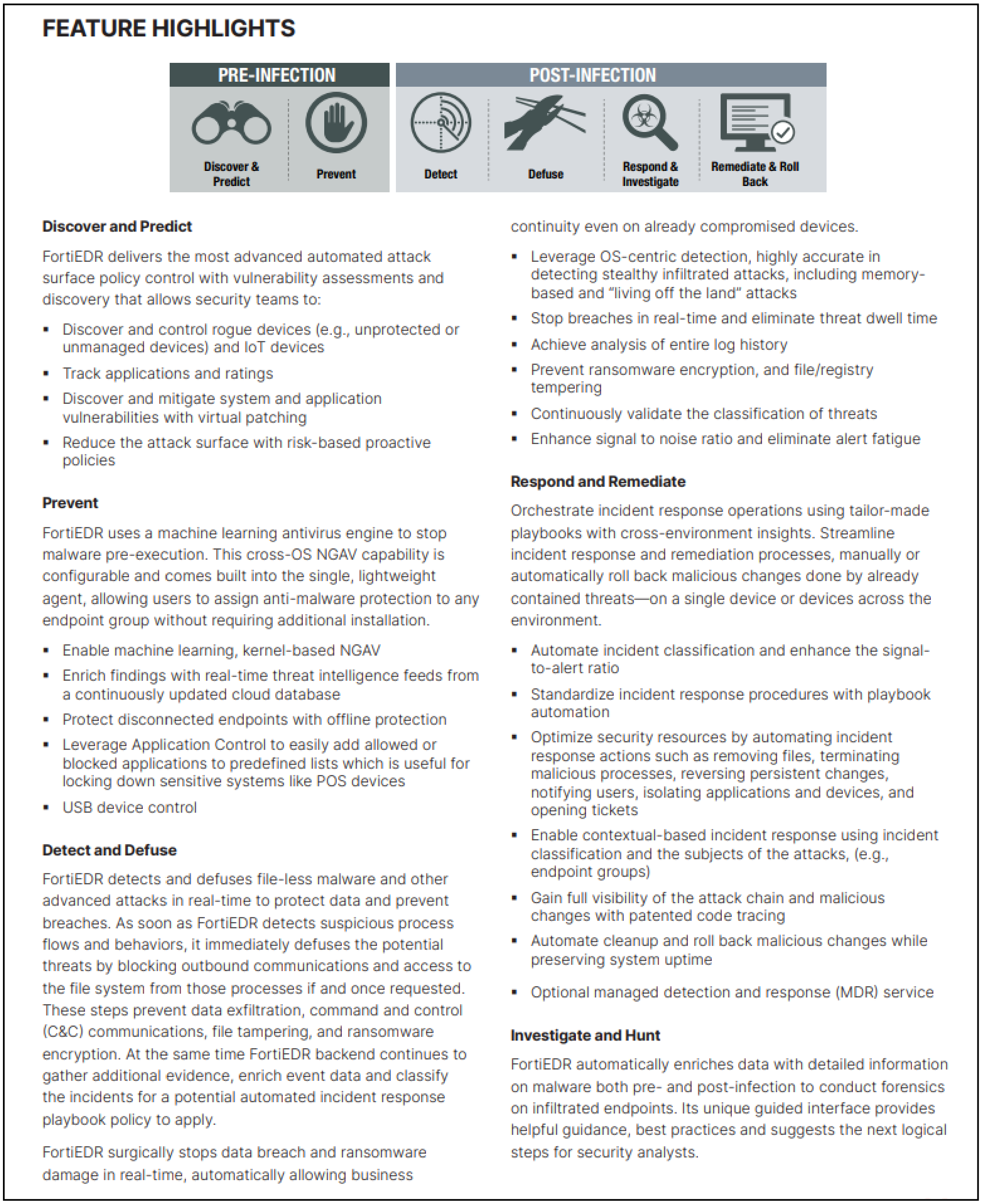
ADVANCED DATA

29

86. Every ’948 Accused Product practices monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of

[29] https://www.youtube.com/watch?v=_DoSSI9fPAk

the application. For example, Fortinet FortiEDR with XDR monitors suspicious process flows and behaviors, application integrity, operating system activities, and network connections.



FEATURE HIGHLIGHTS

Discover and Predict

FortiEDR delivers the most advanced automated attack surface policy control with vulnerability assessments and discovery that allows security teams to:

- Discover and control rogue devices (e.g., unprotected or unmanaged devices) and IoT devices
- Track applications and ratings
- Discover and mitigate system and application vulnerabilities with virtual patching
- Reduce the attack surface with risk-based proactive policies

Prevent

FortiEDR uses a machine learning antivirus engine to stop malware pre-execution. This cross-OS NGAV capability is configurable and comes built into the single, lightweight agent, allowing users to assign anti-malware protection to any endpoint group without requiring additional installation.

- Enable machine learning, kernel-based NGAV
- Enrich findings with real-time threat intelligence feeds from a continuously updated cloud database
- Protect disconnected endpoints with offline protection
- Leverage Application Control to easily add allowed or blocked applications to predefined lists which is useful for locking down sensitive systems like POS devices
- USB device control

Detect and Defuse

FortiEDR detects and defuses file-less malware and other advanced attacks in real-time to protect data and prevent breaches. As soon as FortiEDR detects suspicious process flows and behaviors, it immediately defuses the potential threats by blocking outbound communications and access to the file system from those processes if and once requested. These steps prevent data exfiltration, command and control (C&C) communications, file tampering, and ransomware encryption. At the same time FortiEDR backend continues to gather additional evidence, enrich event data and classify the incidents for a potential automated incident response playbook policy to apply.

FortiEDR surgically stops data breach and ransomware damage in real-time, automatically allowing business continuity even on already compromised devices.

- Leverage OS-centric detection, highly accurate in detecting stealthy infiltrated attacks, including memory-based and "living off the land" attacks
- Stop breaches in real-time and eliminate threat dwell time
- Achieve analysis of entire log history
- Prevent ransomware encryption, and file/registry tempering
- Continuously validate the classification of threats
- Enhance signal to noise ratio and eliminate alert fatigue

Respond and Remediate

Orchestrate incident response operations using tailor-made playbooks with cross-environment insights. Streamline incident response and remediation processes, manually or automatically roll back malicious changes done by already contained threats—on a single device or devices across the environment.

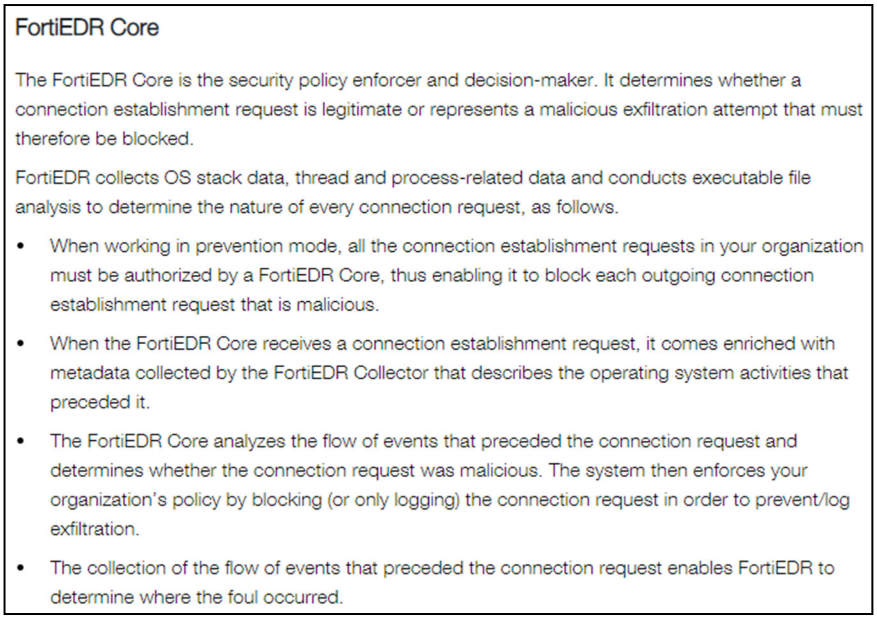
- Automate incident classification and enhance the signal-to-alert ratio
- Standardize incident response procedures with playbook automation
- Optimize security resources by automating incident response actions such as removing files, terminating malicious processes, reversing persistent changes, notifying users, isolating applications and devices, and opening tickets
- Enable contextual-based incident response using incident classification and the subjects of the attacks, (e.g., endpoint groups)
- Gain full visibility of the attack chain and malicious changes with patented code tracing
- Automate cleanup and roll back malicious changes while preserving system uptime
- Optional managed detection and response (MDR) service

Investigate and Hunt

FortiEDR automatically enriches data with detailed information on malware both pre- and post-infection to conduct forensics on infiltrated endpoints. Its unique guided interface provides helpful guidance, best practices and suggests the next logical steps for security analysts.

[30]

[30] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf



FortiEDR Core

The FortiEDR Core is the security policy enforcer and decision-maker. It determines whether a connection establishment request is legitimate or represents a malicious exfiltration attempt that must therefore be blocked.

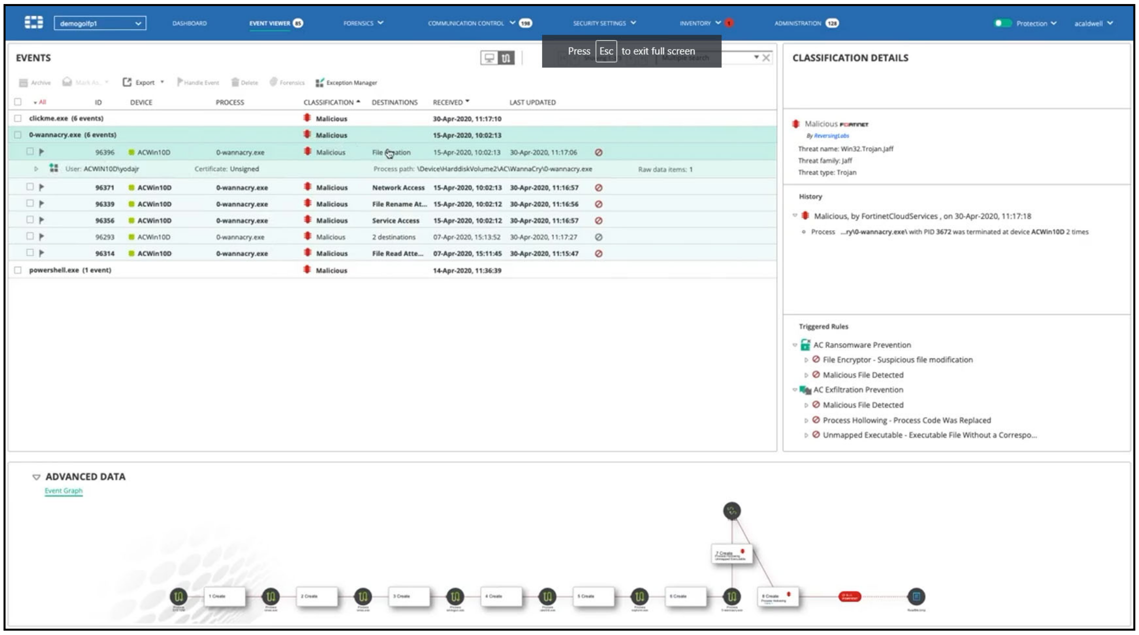
FortiEDR collects OS stack data, thread and process-related data and conducts executable file analysis to determine the nature of every connection request, as follows.

- When working in prevention mode, all the connection establishment requests in your organization must be authorized by a FortiEDR Core, thus enabling it to block each outgoing connection establishment request that is malicious.
- When the FortiEDR Core receives a connection establishment request, it comes enriched with metadata collected by the FortiEDR Collector that describes the operating system activities that preceded it.
- The FortiEDR Core analyzes the flow of events that preceded the connection request and determines whether the connection request was malicious. The system then enforces your organization's policy by blocking (or only logging) the connection request in order to prevent/log exfiltration.
- The collection of the flow of events that preceded the connection request enables FortiEDR to determine where the foul occurred.

[31]

87. Every ’948 Accused Product practices generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor. For example, Fortinet FortiEDR security agents generate behavior based events for determining the real time operational integrity of the application executing on the native computer environment.

[31] https://docs.fortinet.com/document/fortiedr/5.0.0/administration-guide/970632/fortiedr-components



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
User: ACWIN10D\yodajr			Certificate: Unsigned		Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe		Raw data items: 1
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

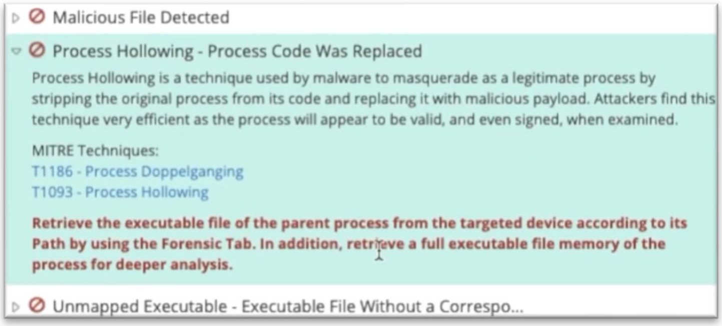
Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

Triggered Rules

- AC Ransomware Prevention
  - File Encryptor - Suspicious file modification
  - Malicious File Detected
- AC Exfiltration Prevention
  - Malicious File Detected
  - Process Hollowing - Process Code Was Replaced
  - Unmapped Executable - Executable File Without a Correspo...

32

88. Every ’948 Accused Product practices correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events. For example, the MITRE ATT&CK framework correlates threat classifications based on the temporal sequence of detected behavioral events.[33]



- Malicious File Detected
- Process Hollowing - Process Code Was Replaced

  Process Hollowing is a technique used by malware to masquerade as a legitimate process by stripping the original process from its code and replacing it with malicious payload. Attackers find this technique very efficient as the process will appear to be valid, and even signed, when examined.

  MITRE Techniques:
  T1186 - Process Doppelganging
  T1093 - Process Hollowing

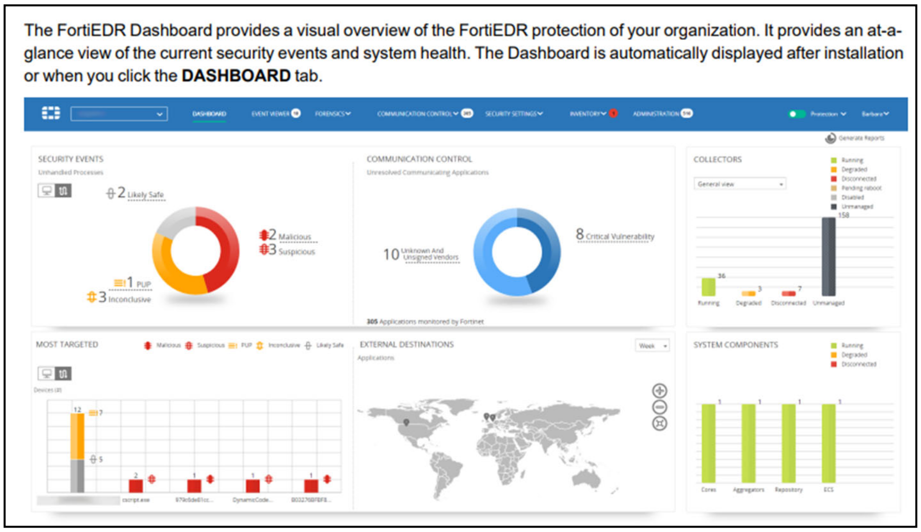
  Retrieve the executable file of the parent process from the targeted device according to its Path by using the Forensic Tab. In addition, retrieve a full executable file memory of the process for deeper analysis.
- Unmapped Executable - Executable File Without a Correspo...

34

89. Every ’948 Accused Product practices displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status

[32] https://www.youtube.com/watch?v=_DoSSI9fPAk
[33] *Id*.
[34] *Id*.

indications for operational integrity of the application. For example, Fortinet FortiEDR includes several display options for showing real-time status indications for the operational integrity of the application.[35]


The FortiEDR Dashboard provides a visual overview of the FortiEDR protection of your organization. It provides an at-a-glance view of the current security events and system health. The Dashboard is automatically displayed after installation or when you click the **DASHBOARD** tab.

36

90. Defendant has and continues to indirectly infringe one or more claims of the '948 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as '948 Accused Products (*e.g.*, products incorporating the application behavioral analysis feature).

91. Defendant, with knowledge that these products, or the use thereof, infringe the '948 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the '948 Patent by providing these products to others, including customers and end-users, for use in an infringing manner, as well as

[35] *Id.*
[36] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

providing demonstrations, training, instruction courses, instruction manuals, installation manuals, and customer service that instruct end-users to use the products in an infringing manner.[37]

92. Defendant encourages and induces its users and customers of the ’948 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[38]

93. Defendant further encourages and induces its customers and users to use the infringing Falcon Platform by providing directions for and encouraging FortiEDR Collector software to be installed on individual endpoint computers.[39]

94. Defendant induced and is currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’948 Patent, but while remaining willfully blind to the infringement.

95. Taasera Licensing has suffered damages as a result of Defendant’s direct and indirect infringement of the ’948 Patent in an amount to be proved at trial.

96. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’948 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

[37] https://www.fortinet.com/products/endpoint-security/fortiedr/demo; https://training.fortinet.com/local/staticpage/view.php?page=library_fortiedr; https://training.fortinet.com/; https://www.fortinet.com/products/endpoint-security/fortiedr; https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

[38] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[39] https://docs.fortinet.com/document/fortiedr/5.1.0/administration-guide/186029/installing-fortiedr-collectors

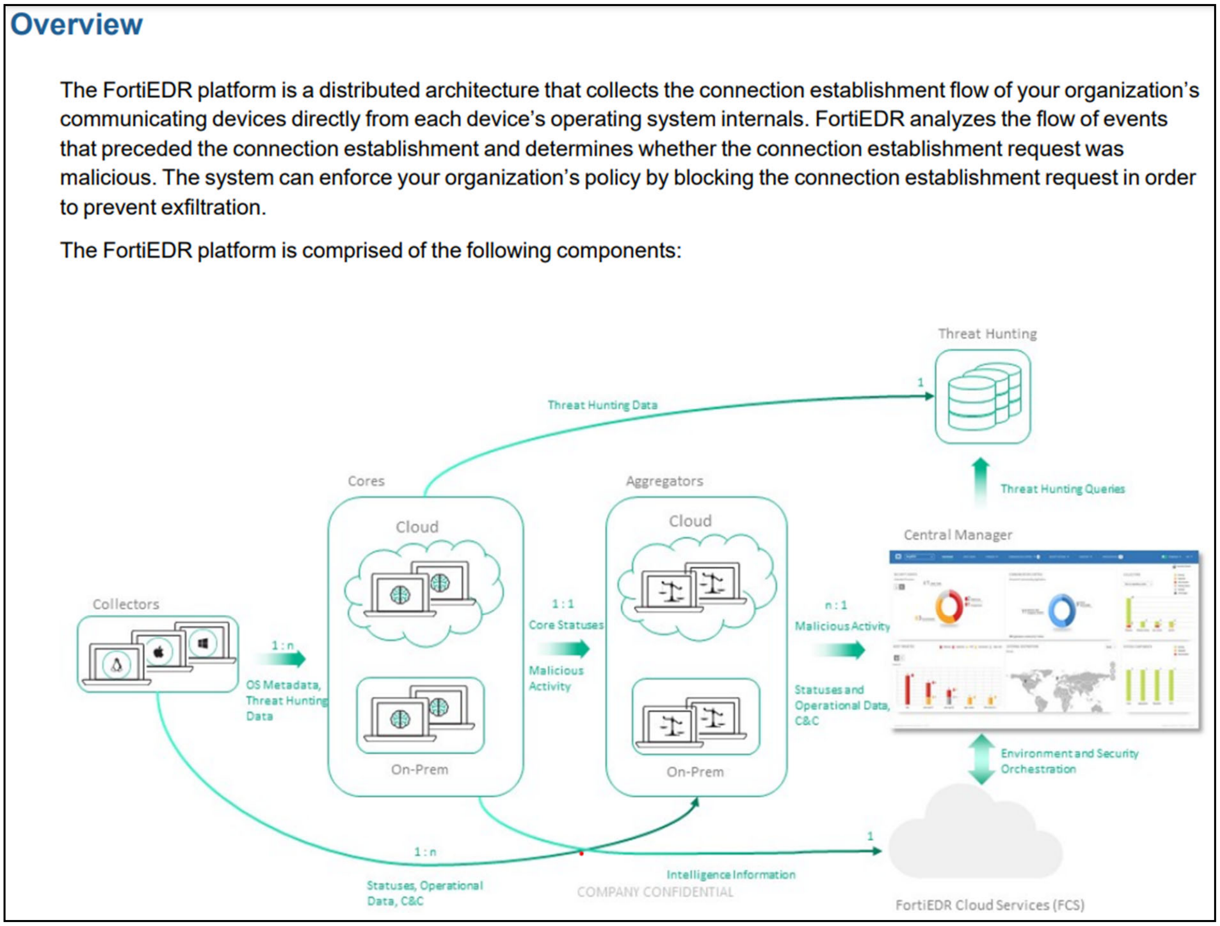
COUNT V
(Infringement of the ’616 Patent)

97. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

98. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’616 Patent.

99. Defendant has and continues to directly infringe at least claim 1 of the ’616 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’616 Patent. Such products incorporate the behavioral analysis feature and include at least the Fortinet FortiEDR (the “’616 Accused Products”) which practice a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising: sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime; receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime; analyzing, by the trust orchestration server, the received endpoint events; receiving, by the trust orchestration server, third-party network endpoint assessments; generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments; correlating, by the trust orchestration server, the received endpoint events and the generated temporal events; and generating, by the trust orchestration server, an integrity profile for the system.

100. Every ’616 Accused Product practices a method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server. For example, Fortinet FortiEDR comprises the Collectors, Cores and Aggregators and a Central Manager to provide operational integrity of a system.



Overview

The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization’s communicating devices directly from each device’s operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization’s policy by blocking the connection establishment request in order to prevent exfiltration.

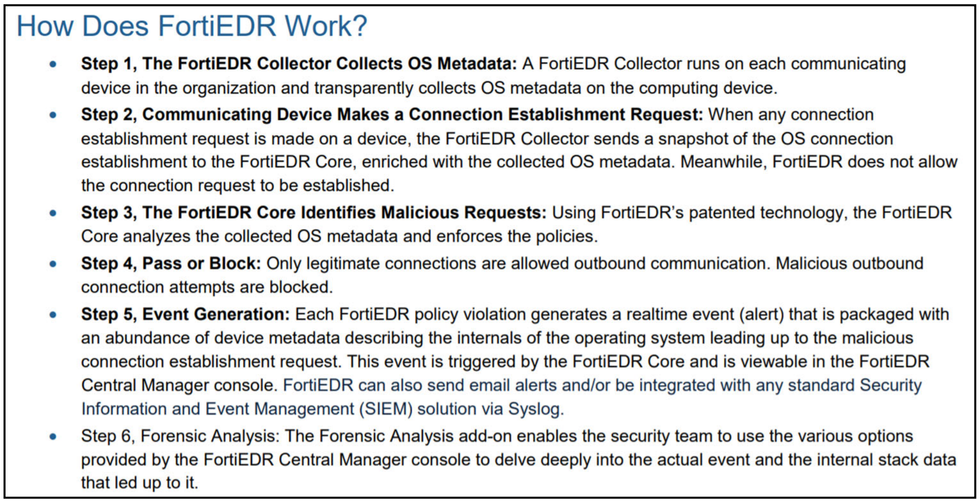
The FortiEDR platform is comprised of the following components:

[40]

101. Every ’616 Accused Product practices sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored

[40] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

device and applications executing on the monitored device at runtime. For example, the security agents send events, context, and status information.



How Does FortiEDR Work?

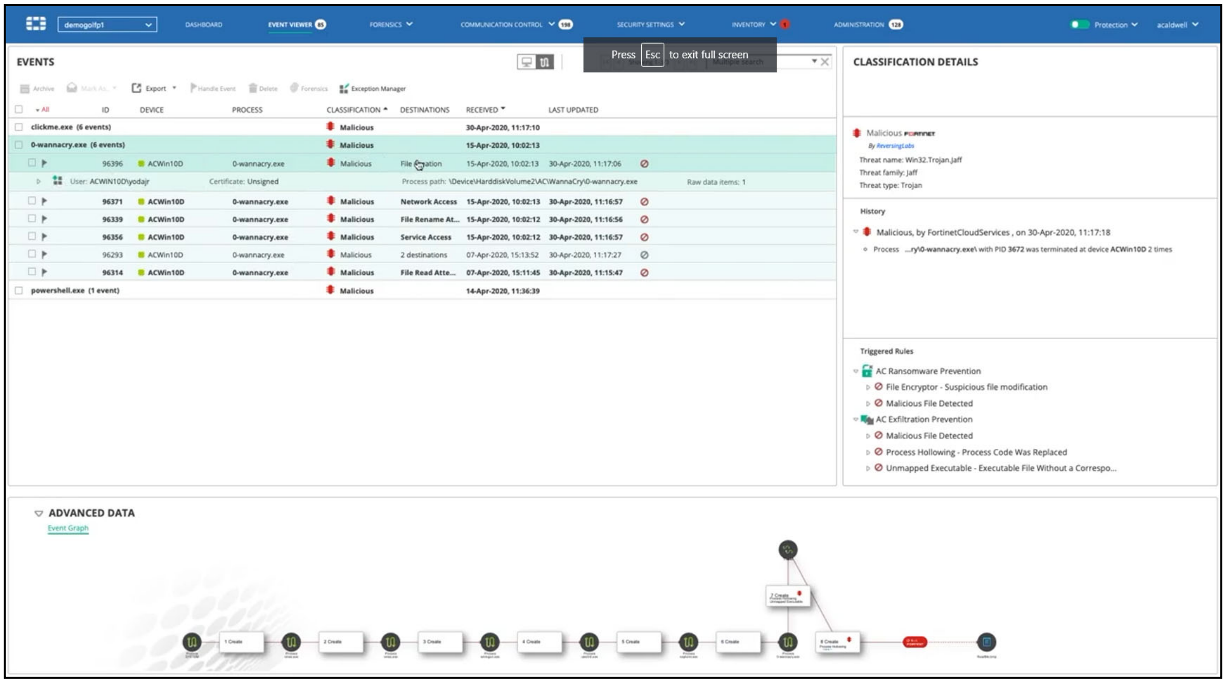
- **Step 1, The FortiEDR Collector Collects OS Metadata:** A FortiEDR Collector runs on each communicating device in the organization and transparently collects OS metadata on the computing device.
- **Step 2, Communicating Device Makes a Connection Establishment Request:** When any connection establishment request is made on a device, the FortiEDR Collector sends a snapshot of the OS connection establishment to the FortiEDR Core, enriched with the collected OS metadata. Meanwhile, FortiEDR does not allow the connection request to be established.
- **Step 3, The FortiEDR Core Identifies Malicious Requests:** Using FortiEDR's patented technology, the FortiEDR Core analyzes the collected OS metadata and enforces the policies.
- **Step 4, Pass or Block:** Only legitimate connections are allowed outbound communication. Malicious outbound connection attempts are blocked.
- **Step 5, Event Generation:** Each FortiEDR policy violation generates a realtime event (alert) that is packaged with an abundance of device metadata describing the internals of the operating system leading up to the malicious connection establishment request. This event is triggered by the FortiEDR Core and is viewable in the FortiEDR Central Manager console. FortiEDR can also send email alerts and/or be integrated with any standard Security Information and Event Management (SIEM) solution via Syslog.
- Step 6, Forensic Analysis: The Forensic Analysis add-on enables the security team to use the various options provided by the FortiEDR Central Manager console to delve deeply into the actual event and the internal stack data that led up to it.

[41]

102. Every ’616 Accused Product practices receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime. For example, Fortinet FortiEDR Core (and Central Manager Console) receives dynamic context including endpoint events and the applications executing on the monitored device in runtime.[42]

[41] *Id*.

[42] *Id*.



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
User: ACWIN10D\yodajr			Certificate: Unsigned		Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe		Raw data items: 1
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

Triggered Rules

- AC Ransomware Prevention
  - File Encryptor - Suspicious file modification
  - Malicious File Detected
- AC Exfiltration Prevention
  - Malicious File Detected
  - Process Hollowing - Process Code Was Replaced
  - Unmapped Executable - Executable File Without a Correspo...

ADVANCED DATA

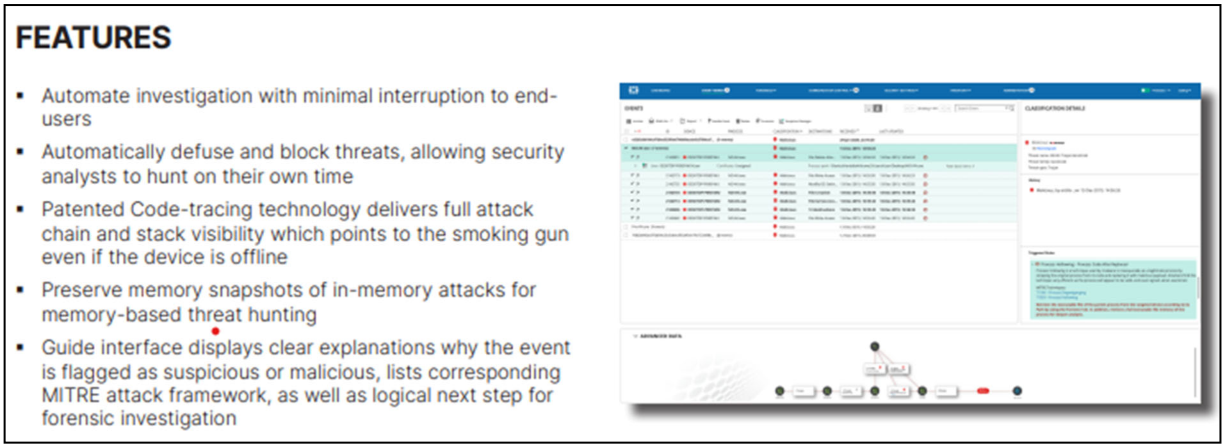
Event Graph

[43]

103. Every ’616 Accused Product practices analyzing, by the trust orchestration server, the received endpoint events. For example, Fortinet FortiEDR Core receives endpoint events (*i.e.*, data related to potential security threats).[44]

104. Every ’616 Accused Product practices receiving, by the trust orchestration server, third-party network endpoint assessments. For example, Fortinet FortiEDR receives MITRE ATT&CK data and other third-party network endpoint assessments.

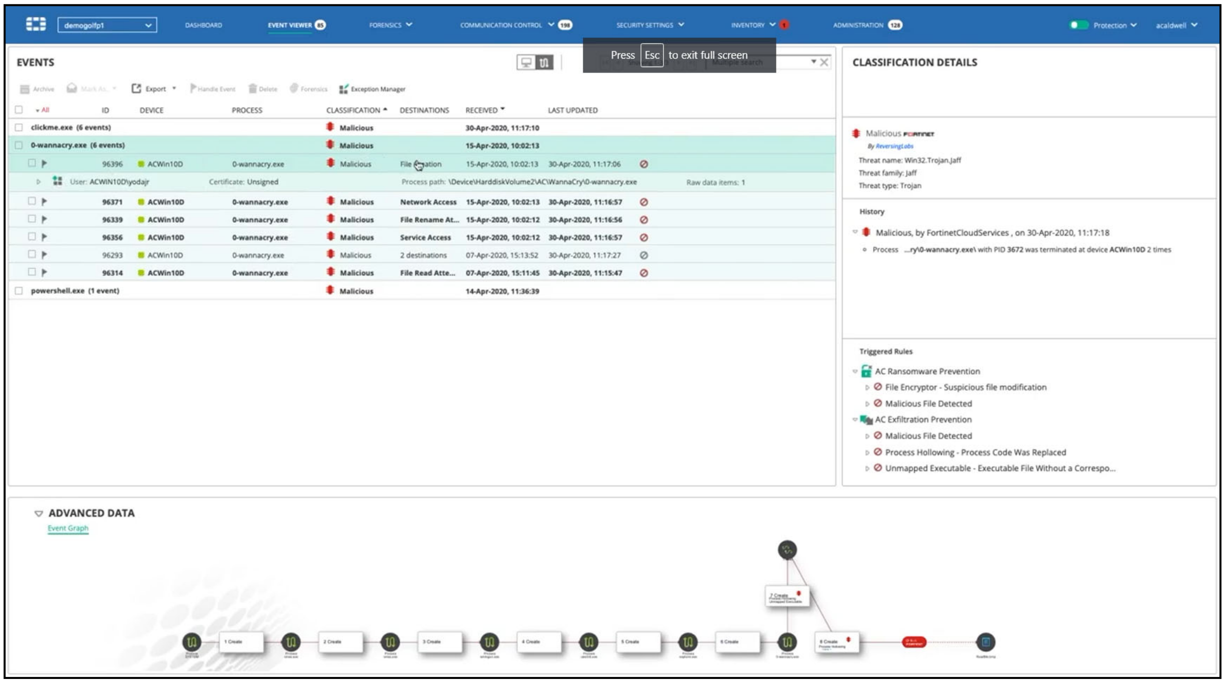
[43] https://www.youtube.com/watch?v=_DoSSI9fPAk
[44] *Id*.



FEATURES

- Automate investigation with minimal interruption to end-users
- Automatically defuse and block threats, allowing security analysts to hunt on their own time
- Patented Code-tracing technology delivers full attack chain and stack visibility which points to the smoking gun even if the device is offline
- Preserve memory snapshots of in-memory attacks for memory-based threat hunting
- Guide interface displays clear explanations why the event is flagged as suspicious or malicious, lists corresponding MITRE attack framework, as well as logical next step for forensic investigation

45



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
	User: ACWIN10D\yodajr		Certificate: Unsigned		Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe		Raw data items: 1
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18

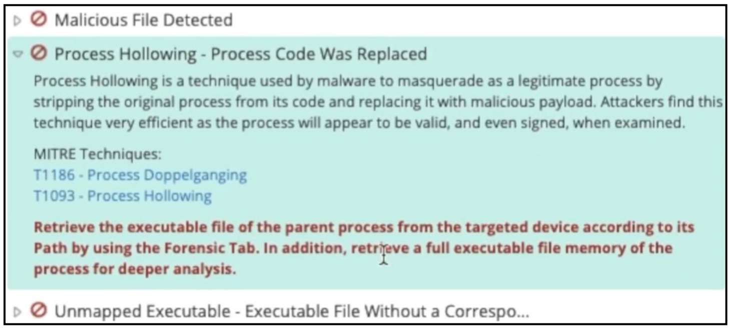
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

Triggered Rules

- AC Ransomware Prevention
  - File Encryptor - Suspicious file modification
  - Malicious File Detected
- AC Exfiltration Prevention
  - Malicious File Detected
  - Process Hollowing - Process Code Was Replaced
  - Unmapped Executable - Executable File Without a Correspo...

ADVANCED DATA

Event Graph



- Malicious File Detected
- Process Hollowing - Process Code Was Replaced

  Process Hollowing is a technique used by malware to masquerade as a legitimate process by stripping the original process from its code and replacing it with malicious payload. Attackers find this technique very efficient as the process will appear to be valid, and even signed, when examined.

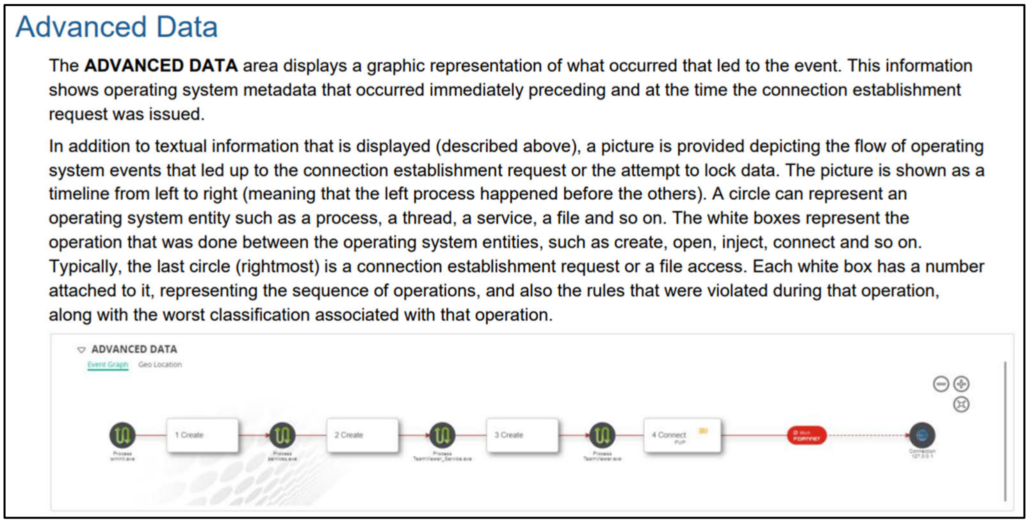
  MITRE Techniques:
  T1186 - Process Doppelganging
  T1093 - Process Hollowing

  Retrieve the executable file of the parent process from the targeted device according to its Path by using the Forensic Tab. In addition, retrieve a full executable file memory of the process for deeper analysis.
- Unmapped Executable - Executable File Without a Correspo...

46

[45] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf
[46] https://www.youtube.com/watch?v=_DoSSI9fPAk

105. Every ’616 Accused Product practices generating, by the trust orchestration server, temporal events based at least in part on analyzing the third-party network endpoint assessments. For example, Fortinet FortiEDR generates temporal events (e.g., classifications) based at least in part on analyzing the third-party network endpoint assessments (*e.g.*, MITRE ATT&CK tactics and techniques).[47]

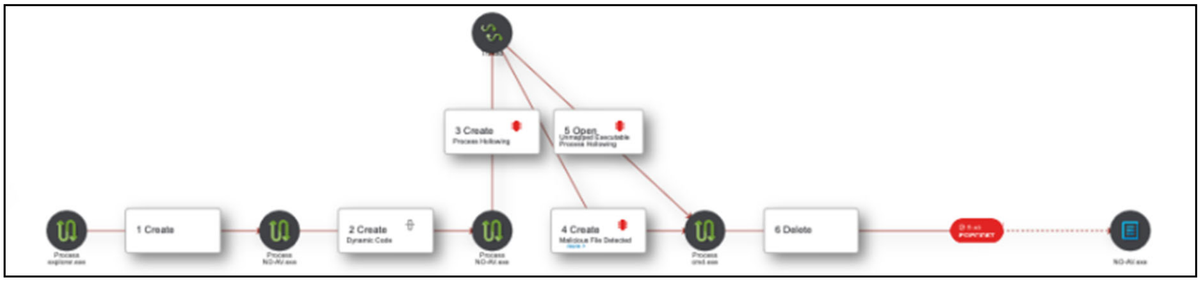


Advanced Data

The **ADVANCED DATA** area displays a graphic representation of what occurred that led to the event. This information shows operating system metadata that occurred immediately preceding and at the time the connection establishment request was issued.

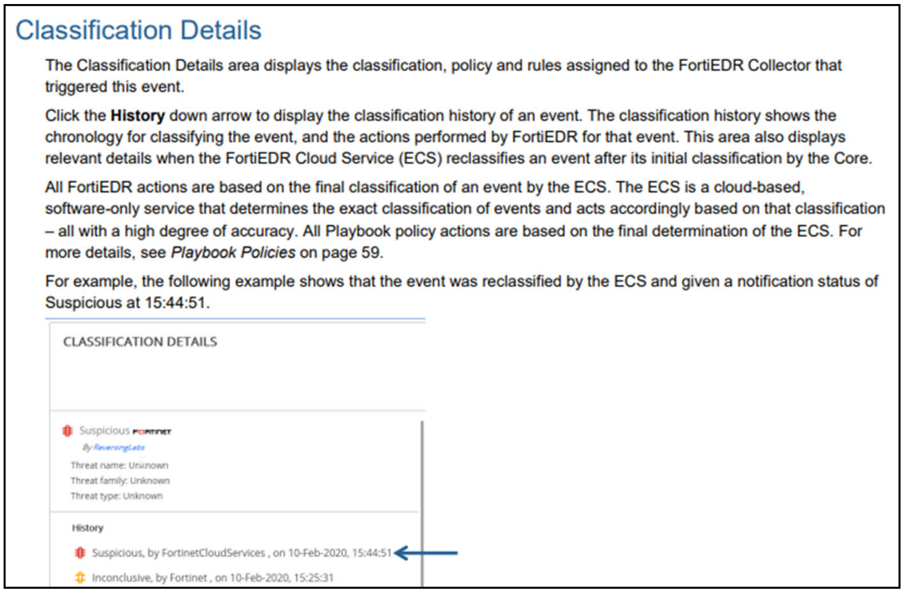
In addition to textual information that is displayed (described above), a picture is provided depicting the flow of operating system events that led up to the connection establishment request or the attempt to lock data. The picture is shown as a timeline from left to right (meaning that the left process happened before the others). A circle can represent an operating system entity such as a process, a thread, a service, a file and so on. The white boxes represent the operation that was done between the operating system entities, such as create, open, inject, connect and so on. Typically, the last circle (rightmost) is a connection establishment request or a file access. Each white box has a number attached to it, representing the sequence of operations, and also the rules that were violated during that operation, along with the worst classification associated with that operation.

48



49

[47] *Id.*
[48] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf
[49] https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiedr.pdf



Classification Details

The Classification Details area displays the classification, policy and rules assigned to the FortiEDR Collector that triggered this event.

Click the **History** down arrow to display the classification history of an event. The classification history shows the chronology for classifying the event, and the actions performed by FortiEDR for that event. This area also displays relevant details when the FortiEDR Cloud Service (ECS) reclassifies an event after its initial classification by the Core.

All FortiEDR actions are based on the final classification of an event by the ECS. The ECS is a cloud-based, software-only service that determines the exact classification of events and acts accordingly based on that classification – all with a high degree of accuracy. All Playbook policy actions are based on the final determination of the ECS. For more details, see *Playbook Policies* on page 59.

For example, the following example shows that the event was reclassified by the ECS and given a notification status of Suspicious at 15:44:51.

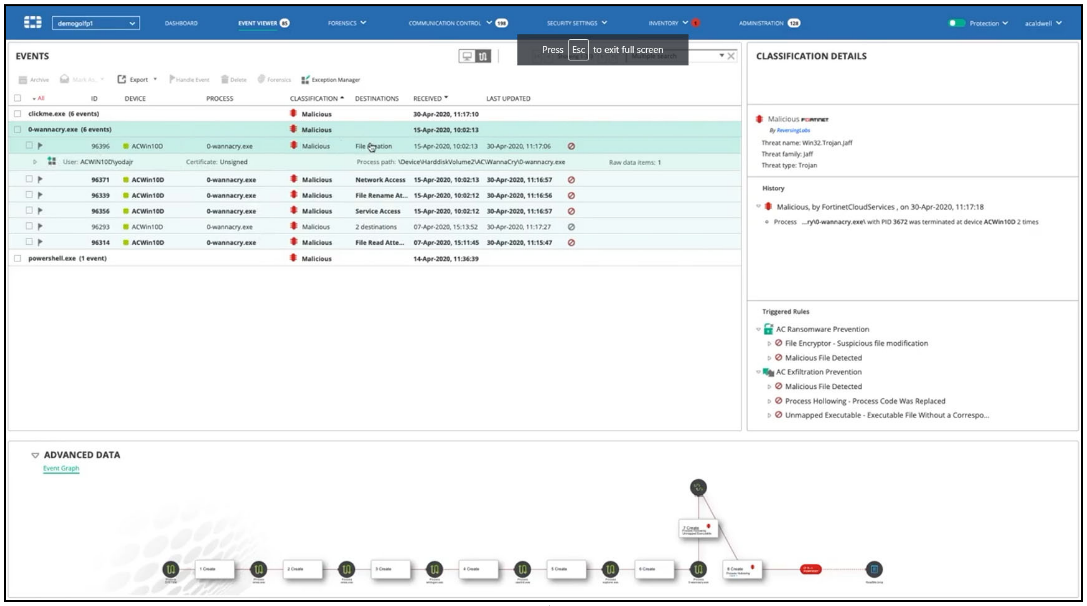
CLASSIFICATION DETAILS

Suspicious FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History
Suspicious, by FortinetCloudServices , on 10-Feb-2020, 15:44:51
Inconclusive, by Fortinet , on 10-Feb-2020, 15:25:31

50

106. Every ’616 Accused Product practices correlating, by the trust orchestration server, the received endpoint events and the generated temporal events. For example, Fortinet FortiEDR correlates the received endpoint events and the generated temporal events (*e.g.*, classification data).



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

User: ACWIN10D\yodajr Certificate: Unsigned Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe Raw data items: 1

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History
Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

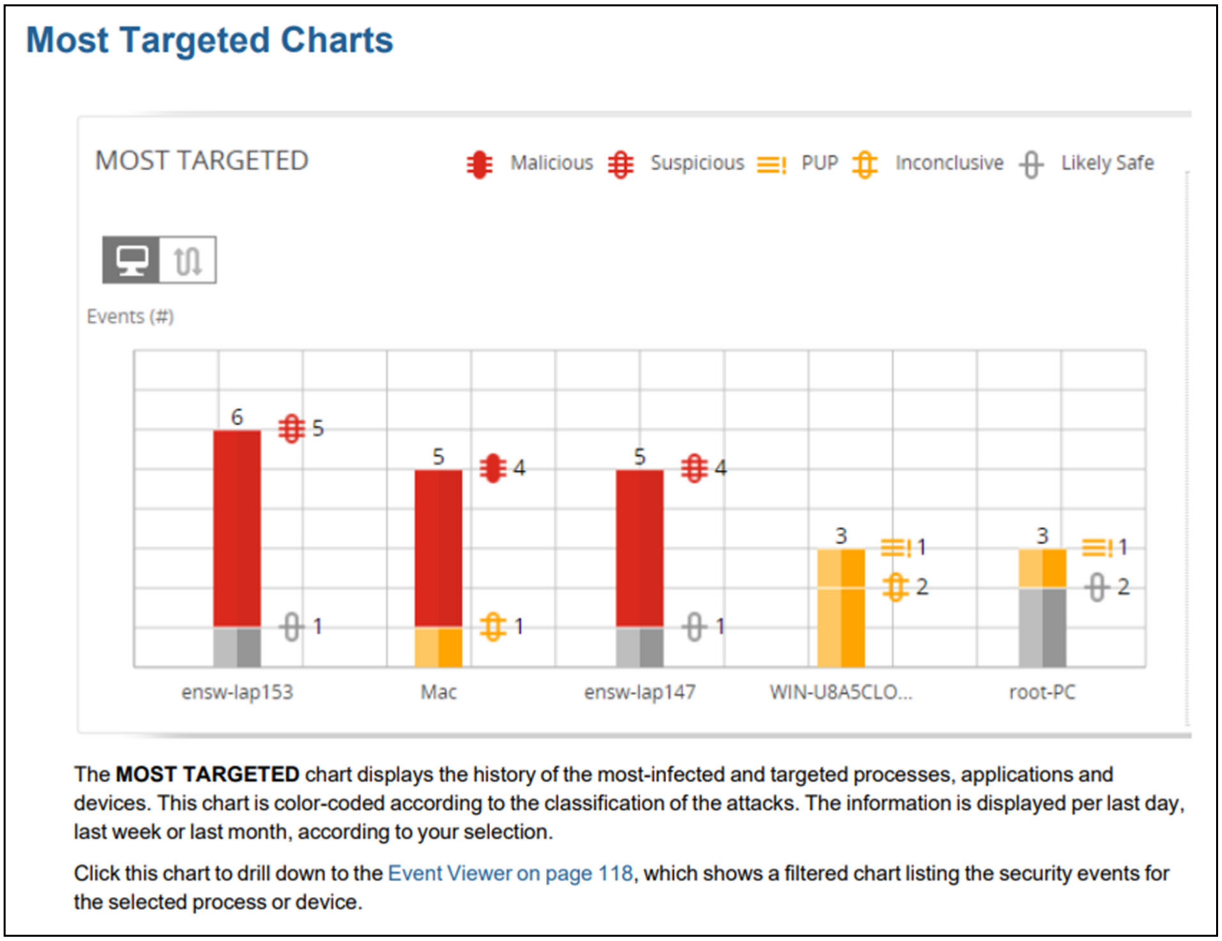
Triggered Rules
AC Ransomware Prevention
File Encryptor - Suspicious file modification
Malicious File Detected
AC Exfiltration Prevention
Malicious File Detected
Process Hollowing - Process Code Was Replaced
Unmapped Executable - Executable File Without a Correspo...

ADVANCED DATA
Event Graph

51

[50] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf
[51] https://www.youtube.com/watch?v=_DoSSI9fPAk

107. Every ’616 Accused Product practices generating, by the trust orchestration server, an integrity profile for the system. For example, Fortinet FortiEDR generates an integrity profile for the system in displaying “Most Targeted Charts.”



Most Targeted Charts

The **MOST TARGETED** chart displays the history of the most-infected and targeted processes, applications and devices. This chart is color-coded according to the classification of the attacks. The information is displayed per last day, last week or last month, according to your selection.

Click this chart to drill down to the Event Viewer on page 118, which shows a filtered chart listing the security events for the selected process or device.

[52]

108. Defendant has and continues to indirectly infringe one or more claims of the ’616 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include

[52] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

infringing technology, such as ’616 Accused Products (*e.g.*, products incorporating the behavioral analysis and classification features).

109. Defendant, with knowledge that these products, or the use thereof, infringe the ’616 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’616 Patent by providing these products to others, including customers and end-users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, installation manuals, and customer service that instruct end-users to use the products in an infringing manner.[53]

110. Defendant encourages and induces its users and customers of the ’616 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[54]

111. Defendant further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging FortiEDR Collector software to be installed on individual endpoint computers.[55]

112. Defendant induced and is currently inducing infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that

[53] https://www.fortinet.com/products/endpoint-security/fortiedr/demo; https://training.fortinet.com/local/staticpage/view.php?page=library_fortiedr; https://training.fortinet.com/; https://www.fortinet.com/products/endpoint-security/fortiedr; https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

[54] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[55] https://docs.fortinet.com/document/fortiedr/5.1.0/administration-guide/186029/installing-fortiedr-collectors

there was a high probability that others, including end- users, infringe the ’616 Patent, but while remaining willfully blind to the infringement.

113. Taasera Licensing has suffered damages as a result of Defendant’s direct and indirect infringement of the ’616 Patent in an amount to be proved at trial.

114. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’616 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT VI
(Infringement of the ’634 Patent)

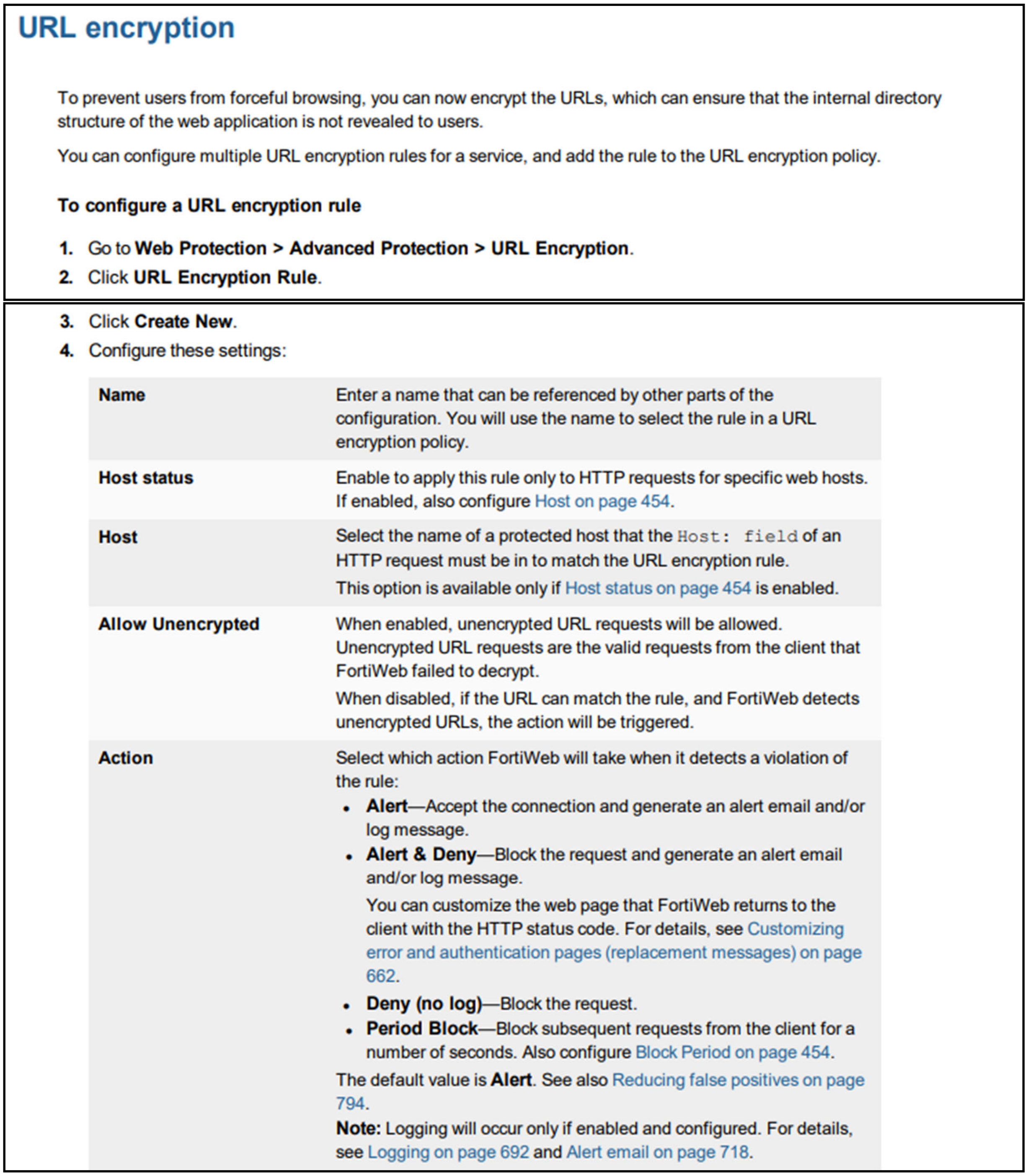
115. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

116. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’634 Patent.

117. Defendant has and continues to directly infringe at least claim 1 of the ’634 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’634 Patent. Such products incorporate the URL Encryption feature and include at least Fortinet Fortiweb (the “’634 Accused Products”) which resides on a computer and a computer readable hardware storage device, said storage device containing instructions which, upon being executed by the computer, implements a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); evaluating, by the computer, the URL to determine whether encryption of none, part, or all of the URL is required; determining by the computer, that the requested resource is available and in

response, locating, by the computer, the requested resource contained in the resource request; and determining, by the computer, whether encryption is required for none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request.

118. Every ’634 Accused Product implements a method for restricting access to information transmitted over a computing network. For example, the Fortinet Fortiweb performs URL encryption.



URL encryption

To prevent users from forceful browsing, you can now encrypt the URLs, which can ensure that the internal directory structure of the web application is not revealed to users.

You can configure multiple URL encryption rules for a service, and add the rule to the URL encryption policy.

To configure a URL encryption rule

1. Go to **Web Protection > Advanced Protection > URL Encryption**.
2. Click **URL Encryption Rule**.
3. Click **Create New**.
4. Configure these settings:

Name	Enter a name that can be referenced by other parts of the configuration. You will use the name to select the rule in a URL encryption policy.
Host status	Enable to apply this rule only to HTTP requests for specific web hosts. If enabled, also configure Host on page 454.
Host	Select the name of a protected host that the `Host: field` of an HTTP request must be in to match the URL encryption rule. This option is available only if Host status on page 454 is enabled.
Allow Unencrypted	When enabled, unencrypted URL requests will be allowed. Unencrypted URL requests are the valid requests from the client that FortiWeb failed to decrypt. When disabled, if the URL can match the rule, and FortiWeb detects unencrypted URLs, the action will be triggered.
Action	Select which action FortiWeb will take when it detects a violation of the rule: • **Alert**—Accept the connection and generate an alert email and/or log message. • **Alert & Deny**—Block the request and generate an alert email and/or log message. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see Customizing error and authentication pages (replacement messages) on page 662. • **Deny (no log)**—Block the request. • **Period Block**—Block subsequent requests from the client for a number of seconds. Also configure Block Period on page 454. The default value is **Alert**. See also Reducing false positives on page 794. **Note:** Logging will occur only if enabled and configured. For details, see Logging on page 692 and Alert email on page 718.

[56]

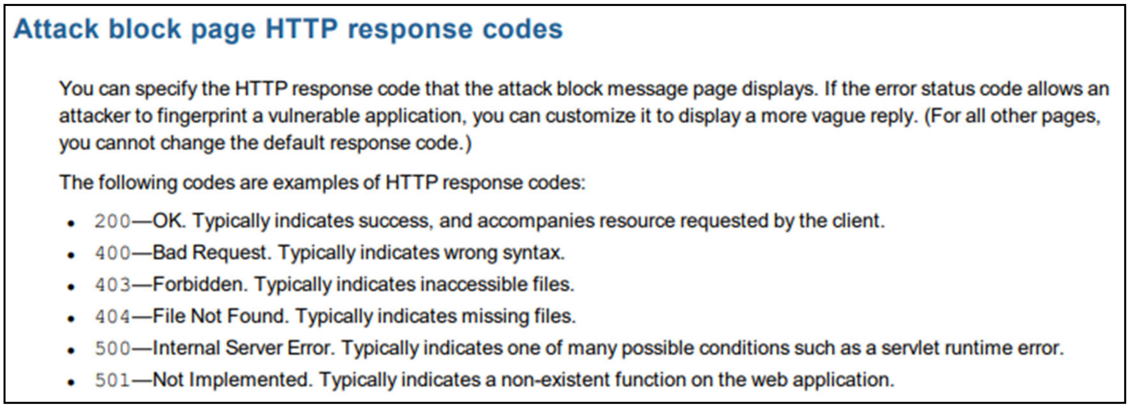
119. Every '634 Accused Product performs receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a

[56] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/5a6875be-586e-11ea-9384-00505692583a/FortiWeb_6.3.1_Administration_Guide.pdf

universal resource locator (URL). For example, Fortinet Fortiweb receives request URLs for resources to be located.[57]

120. Every ’634 Accused Product performs evaluating, by the computer, the URL to determine whether encryption of none, part, or all of the URL is required. For example, Fortinet Fortiweb evaluates whether the URL is listed as a request URL or in an exception list.[58]

121. Every ’634 Accused Product performs determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request. For example, if Fortinet Fortiweb is not able to locate the file, it will return a 404 (file not found) error code. Otherwise, the response is available.



Attack block page HTTP response codes

You can specify the HTTP response code that the attack block message page displays. If the error status code allows an attacker to fingerprint a vulnerable application, you can customize it to display a more vague reply. (For all other pages, you cannot change the default response code.)

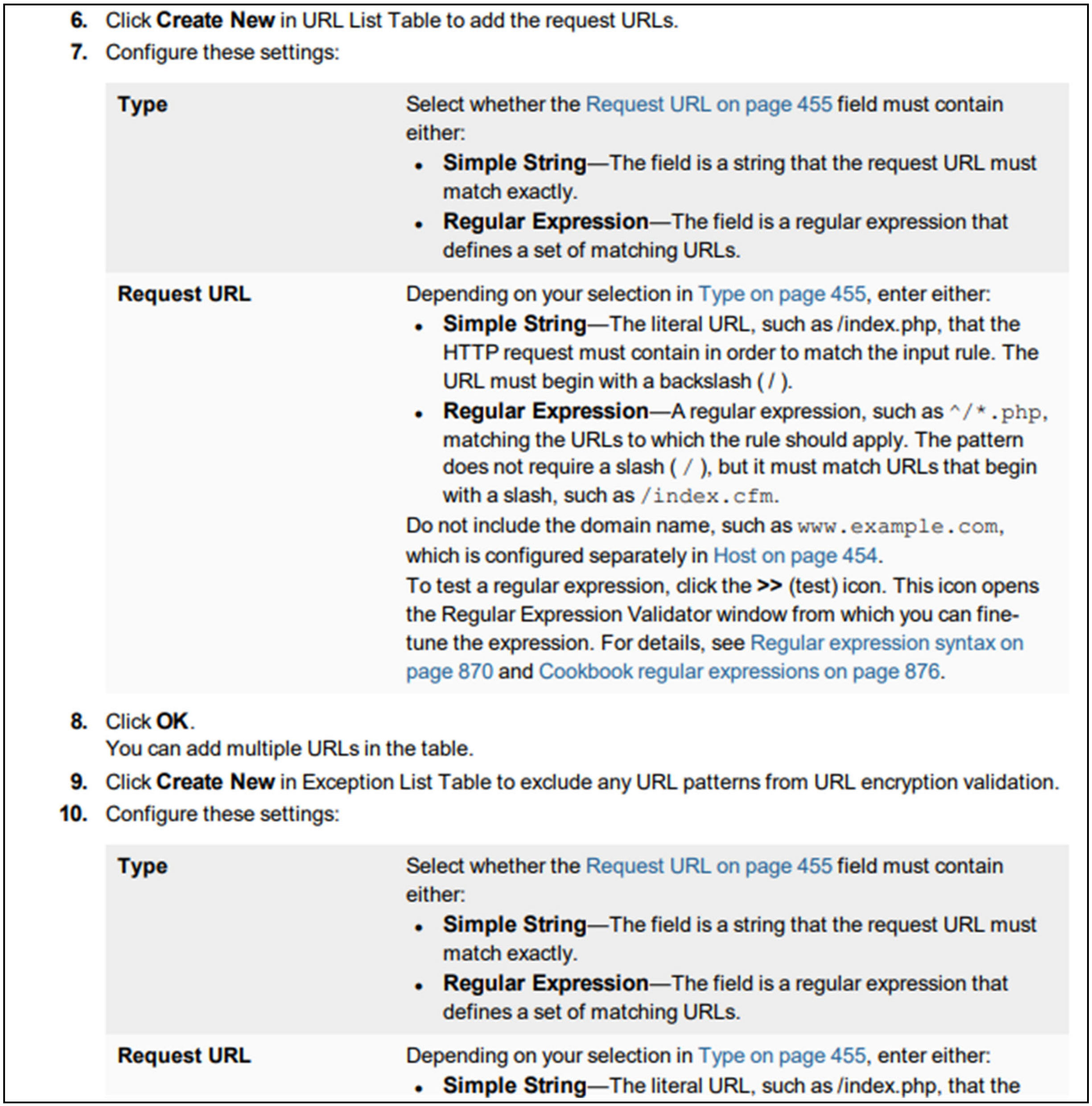
The following codes are examples of HTTP response codes:

- `200`—OK. Typically indicates success, and accompanies resource requested by the client.
- `400`—Bad Request. Typically indicates wrong syntax.
- `403`—Forbidden. Typically indicates inaccessible files.
- `404`—File Not Found. Typically indicates missing files.
- `500`—Internal Server Error. Typically indicates one of many possible conditions such as a servlet runtime error.
- `501`—Not Implemented. Typically indicates a non-existent function on the web application.

[59]

122. Every ’634 Accused Product performs determining, by the computer, whether encryption is required for none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request. For example, Fortinet Fortiweb encrypts all request URLs unless there is a simple string or regular expression exception.

[57] *Id.*
[58] *Id.*
[59] *Id.*



6. Click **Create New** in URL List Table to add the request URLs.
7. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (/). • **Regular Expression**—A regular expression, such as `^/*.php`, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as `/index.cfm`. Do not include the domain name, such as `www.example.com`, which is configured separately in Host on page 454. To test a regular expression, click the **>>** (test) icon. This icon opens the Regular Expression Validator window from which you can fine-tune the expression. For details, see Regular expression syntax on page 870 and Cookbook regular expressions on page 876.

8. Click **OK**.
   You can add multiple URLs in the table.
9. Click **Create New** in Exception List Table to exclude any URL patterns from URL encryption validation.
10. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the

[60]

123. Defendant has and continues to indirectly infringe one or more claims of the ’634 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include

[60] *Id.*

infringing technology, such as ’634 Accused Products (*e.g.*, products incorporating the URL Encryption feature).

124. Defendant, with knowledge that these products, or the use thereof, infringe the ’634 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’634 Patent by providing these products to other, including customers and end-users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, deployment guides, and customer service that instruct customers to use the products in an infringing manner. [61]

125. Defendant encourages and induces its users and customers of the ’634 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security products available on its website, widely advertises those products, provides applications that allow customers and users to access those products, provides training and instructions for deploying and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[62]

126. Fortinet further encourages and induces its customers to use the infringing Fortiweb product by providing directions for deploying and using Fortiweb.[63]

127. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’634 Patent, but while remaining willfully blind to the infringement.

[61] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0

[62] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[63] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0

128. Taasera Licensing has suffered damages as a result of Defendant's direct and indirect infringement of the '634 Patent in an amount to be proved at trial.

129. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '634 Patent, for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT VII
(Infringement of the '997 Patent)

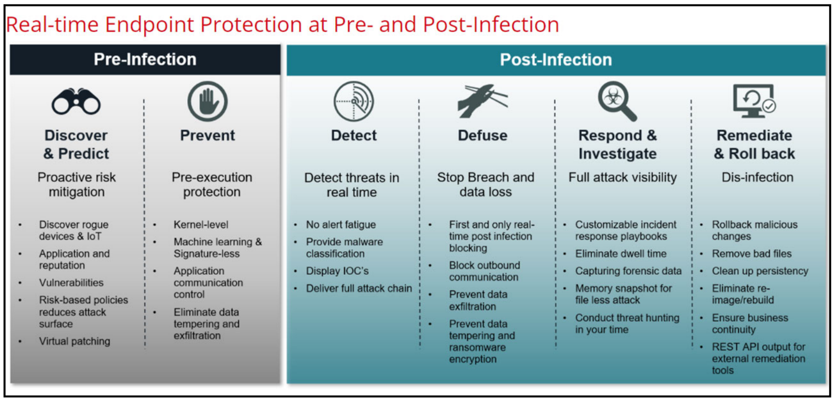
130. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

131. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the '997 Patent.

132. Defendant has and continues to directly infringe at least claim 21 of the '997 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '997 Patent. Such products incorporate the threat classification and remediation features and include at least the Fortinet FortiEDR (the "'997 Accused Products") which practice a method for controlling the operation of an endpoint, comprising: providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; maintaining the plurality of policies in a data store on the computing system; identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services; determining, by the computing system, a compliance state of the endpoint based on the

status information and a plurality of compliance policies in the data store; and initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system.

133. Every '997 Accused Product practices a method for controlling the operation of an endpoint. For example, the Fortinet FortiEDR performs remediation on endpoints.



Real-time Endpoint Protection at Pre- and Post-Infection

Pre-Infection

Discover & Predict

Proactive risk mitigation

- Discover rogue devices & IoT
- Application and reputation
- Vulnerabilities
- Risk-based policies reduces attack surface
- Virtual patching

Prevent

Pre-execution protection

- Kernel-level
- Machine learning & Signature-less
- Application communication control
- Eliminate data tempering and exfiltration

Post-Infection

Detect

Detect threats in real time

- No alert fatigue
- Provide malware classification
- Display IOC's
- Deliver full attack chain

Defuse

Stop Breach and data loss

- First and only real-time post infection blocking
- Block outbound communication
- Prevent data exfiltration
- Prevent data tempering and ransomware encryption

Respond & Investigate

Full attack visibility

- Customizable incident response playbooks
- Eliminate dwell time
- Capturing forensic data
- Memory snapshot for file less attack
- Conduct threat hunting in your time

Remediate & Roll back

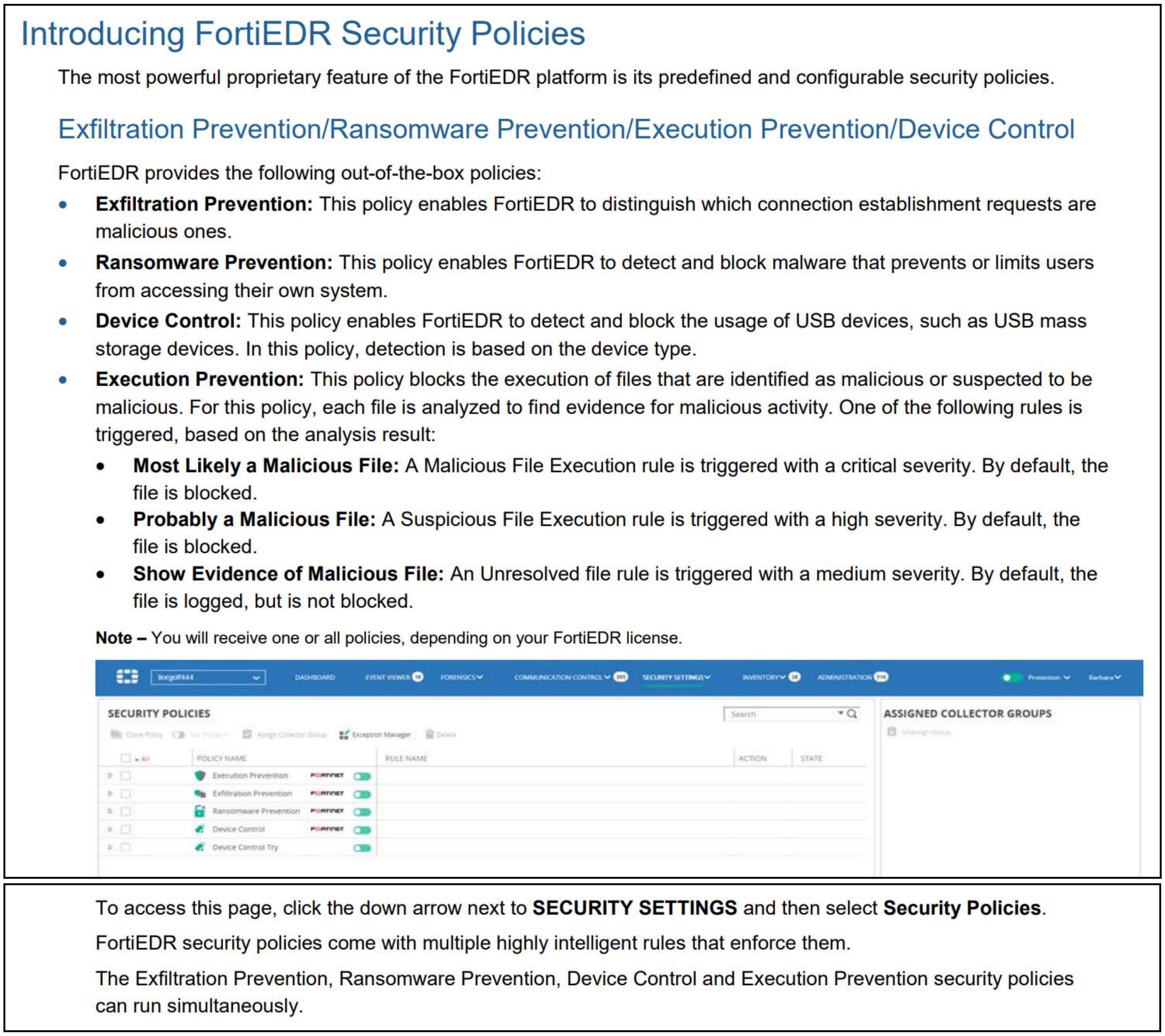
Dis-infection

- Rollback malicious changes
- Remove bad files
- Clean up persistency
- Eliminate re-image/rebuild
- Ensure business continuity
- REST API output for external remediation tools

[64]

134. Every '997 Accused Product practices providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies and maintaining the plurality of policies in a data store on the computing system. For example, Fortinet FortiEDR allows configuration of a plurality of policies (*e.g.*, security policies) at a system remote from the endpoint through a provided user interface which are stored in a data store.

[64] https://www.avfirewalls.com/FortiEDR.asp



Introducing FortiEDR Security Policies

The most powerful proprietary feature of the FortiEDR platform is its predefined and configurable security policies.

Exfiltration Prevention/Ransomware Prevention/Execution Prevention/Device Control

FortiEDR provides the following out-of-the-box policies:

- **Exfiltration Prevention:** This policy enables FortiEDR to distinguish which connection establishment requests are malicious ones.
- **Ransomware Prevention:** This policy enables FortiEDR to detect and block malware that prevents or limits users from accessing their own system.
- **Device Control:** This policy enables FortiEDR to detect and block the usage of USB devices, such as USB mass storage devices. In this policy, detection is based on the device type.
- **Execution Prevention:** This policy blocks the execution of files that are identified as malicious or suspected to be malicious. For this policy, each file is analyzed to find evidence for malicious activity. One of the following rules is triggered, based on the analysis result:
  - **Most Likely a Malicious File:** A Malicious File Execution rule is triggered with a critical severity. By default, the file is blocked.
  - **Probably a Malicious File:** A Suspicious File Execution rule is triggered with a high severity. By default, the file is blocked.
  - **Show Evidence of Malicious File:** An Unresolved file rule is triggered with a medium severity. By default, the file is logged, but is not blocked.

Note – You will receive one or all policies, depending on your FortiEDR license.

All	POLICY NAME			RULE NAME	ACTION	STATE
□	Execution Prevention	FORTINET	●			
□	Exfiltration Prevention	FORTINET	●			
□	Ransomware Prevention	FORTINET	●			
□	Device Control	FORTINET	●			
□	Device Control Try		●			

To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.

FortiEDR security policies come with multiple highly intelligent rules that enforce them.

The Exfiltration Prevention, Ransomware Prevention, Device Control and Execution Prevention security policies can run simultaneously.

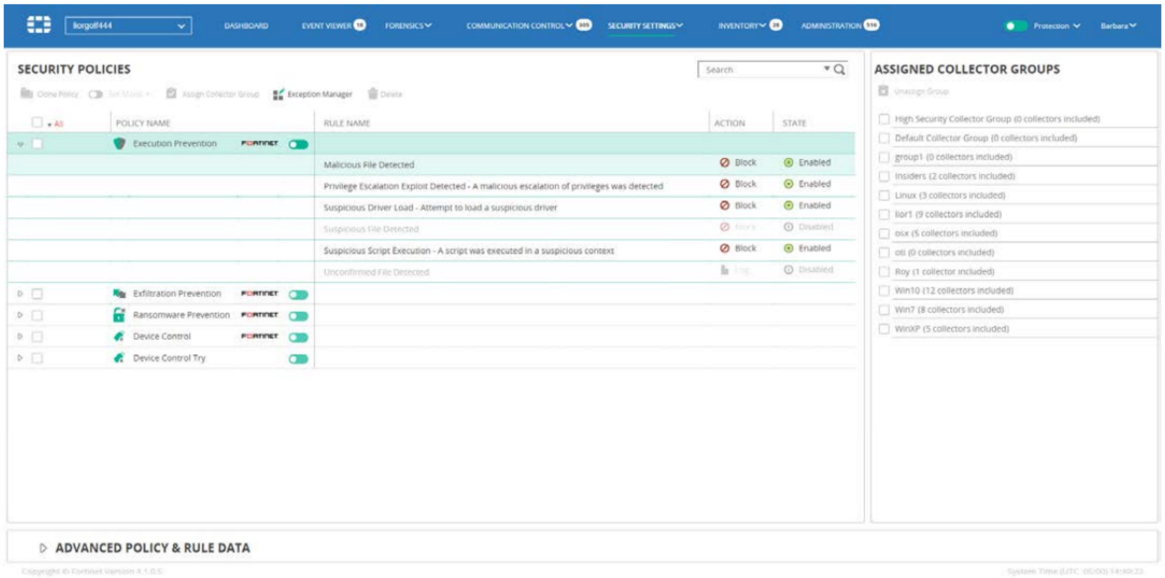
[65]

135. Every ’997 Accused Product practices identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor. For example, Fortinet FortiEDR security policies identify, from the plurality of polices, operating conditions on the endpoint (such as the operating conditions listed in the “rules”) to monitor.

[65] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf

Security Policies Page

The **SECURITY POLICIES** page displays a row for each security policy. Each policy row can be expanded to show the rules that it contains, as shown below. To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.



SECURITY POLICIES

All	POLICY NAME	RULE NAME	ACTION	STATE
□	Execution Prevention FORTINET			
		Malicious File Detected	Block	Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
		Suspicious File Detected	Block	Disabled
		Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
		Unconfirmed File Detected	Log	Disabled
□	Exfiltration Prevention FORTINET			
□	Ransomware Prevention FORTINET			
□	Device Control FORTINET			
□	Device Control Try			

ASSIGNED COLLECTOR GROUPS

- □ High Security Collector Group (0 collectors included)
- □ Default Collector Group (0 collectors included)
- □ group1 (0 collectors included)
- □ Insiders (2 collectors included)
- □ Linux (3 collectors included)
- □ lior1 (9 collectors included)
- □ osx (5 collectors included)
- □ oti (0 collectors included)
- □ Roy (1 collector included)
- □ Win10 (12 collectors included)
- □ Win7 (8 collectors included)
- □ WinXP (5 collectors included)

FortiEDR is provided out-of-the-box with several predefined security policies (depending on your license), ready for you to get started. By default, all policies are set to **Simulation** mode (meaning that they ***only*** log and ***do not block***) and show the FORTINET logo. This page also enables you to define additional policies.

Exfiltration prevention policies are marked with the icon, ransomware prevention policies are marked with the icon, execution prevention policies are marked with the icon and device control policies are marked with the icon.

The following information is defined per security policy:

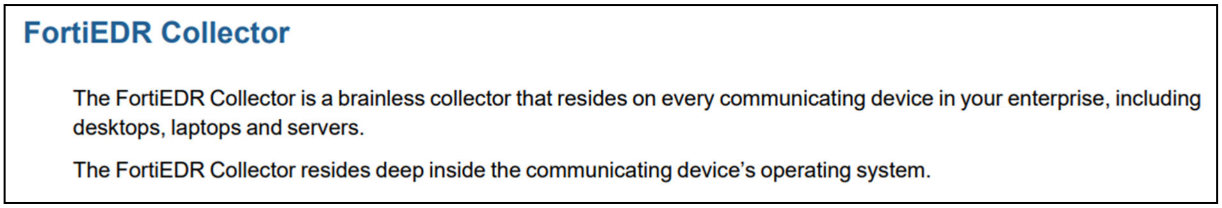
Note – Only the **ACTION** (described below) and the **STATE** (Enabled/Disabled) column of a rule can be changed by you.

- **POLICY NAME:** The policy name appears in the leftmost column. The policy name is defined when the policy is created. The name of the **Default Policy** cannot be changed.
- **RULE NAME:** FortiEDR's proprietary rules come predefined and are the primary component of FortiEDR's proprietary security solution. This column displays a short description for the purpose of this rule.

[66]

136. Every ’997 Accused Product practices configuring one or more software services on the endpoint to monitor the plurality of operating conditions. For example, Fortinet FortiEDR configures the FortiEDR Collectors to monitor the plurality of operating conditions (*e.g.*, operating system metadata).

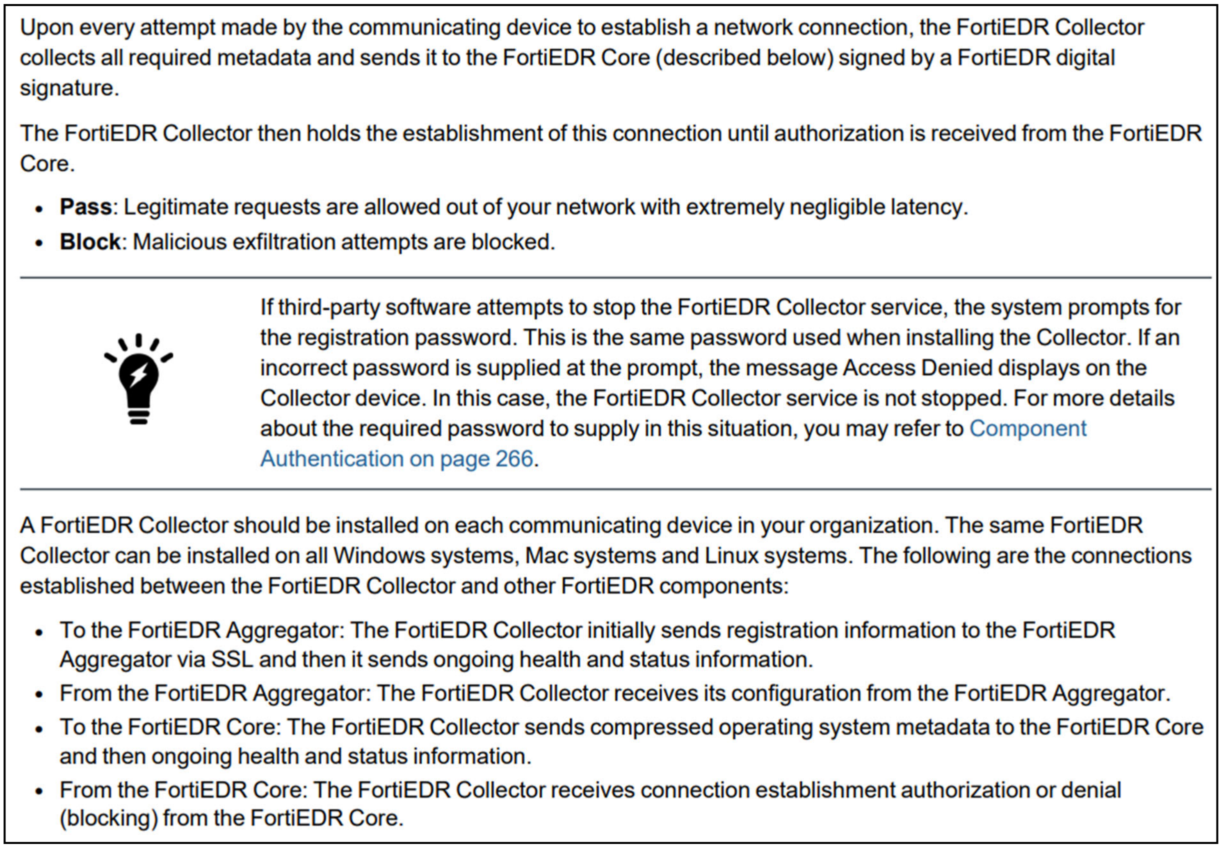
[66] *Id.*



FortiEDR Collector

The FortiEDR Collector is a brainless collector that resides on every communicating device in your enterprise, including desktops, laptops and servers.

The FortiEDR Collector resides deep inside the communicating device's operating system.



Upon every attempt made by the communicating device to establish a network connection, the FortiEDR Collector collects all required metadata and sends it to the FortiEDR Core (described below) signed by a FortiEDR digital signature.

The FortiEDR Collector then holds the establishment of this connection until authorization is received from the FortiEDR Core.

- **Pass**: Legitimate requests are allowed out of your network with extremely negligible latency.
- **Block**: Malicious exfiltration attempts are blocked.

If third-party software attempts to stop the FortiEDR Collector service, the system prompts for the registration password. This is the same password used when installing the Collector. If an incorrect password is supplied at the prompt, the message Access Denied displays on the Collector device. In this case, the FortiEDR Collector service is not stopped. For more details about the required password to supply in this situation, you may refer to Component Authentication on page 266.

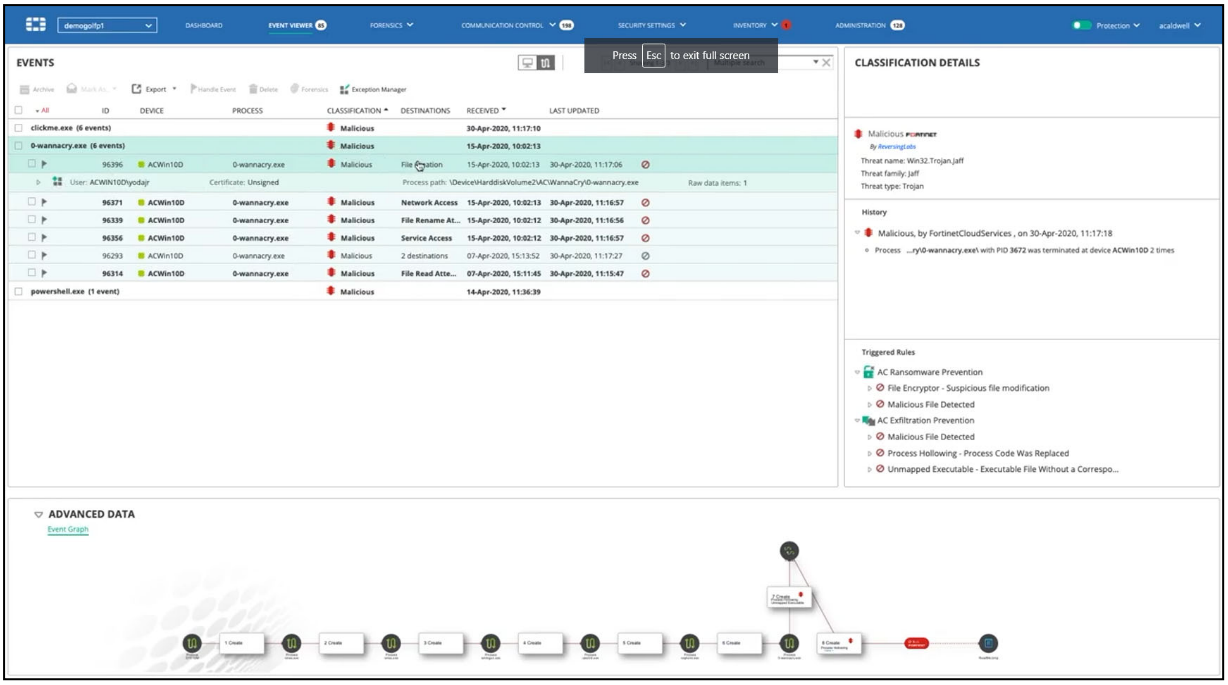
A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows systems, Mac systems and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- To the FortiEDR Aggregator: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health and status information.
- From the FortiEDR Aggregator: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.
- To the FortiEDR Core: The FortiEDR Collector sends compressed operating system metadata to the FortiEDR Core and then ongoing health and status information.
- From the FortiEDR Core: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

[67]

137. Every '997 Accused Product practices receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services. For example, FortiEDR receives events, gathered by the one or more software services (*e.g.*, FortiEDR Collectors). [68]

[67] *Id.*
[68] *Id.*



EVENTS

☐ All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED	
☐ clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10		
☐ 0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13		
☐	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06	⊘
User: ACWIN10D\yodajr			Certificate: Unsigned		Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe			Raw data items: 1
☐	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57	⊘
☐	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56	⊘
☐	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57	⊘
☐	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27	⊘
☐	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47	⊘
☐ powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39		

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

Triggered Rules

- AC Ransomware Prevention
  - ⊘ File Encryptor - Suspicious file modification
  - ⊘ Malicious File Detected
- AC Exfiltration Prevention
  - ⊘ Malicious File Detected
  - ⊘ Process Hollowing - Process Code Was Replaced
  - ⊘ Unmapped Executable - Executable File Without a Correspo...

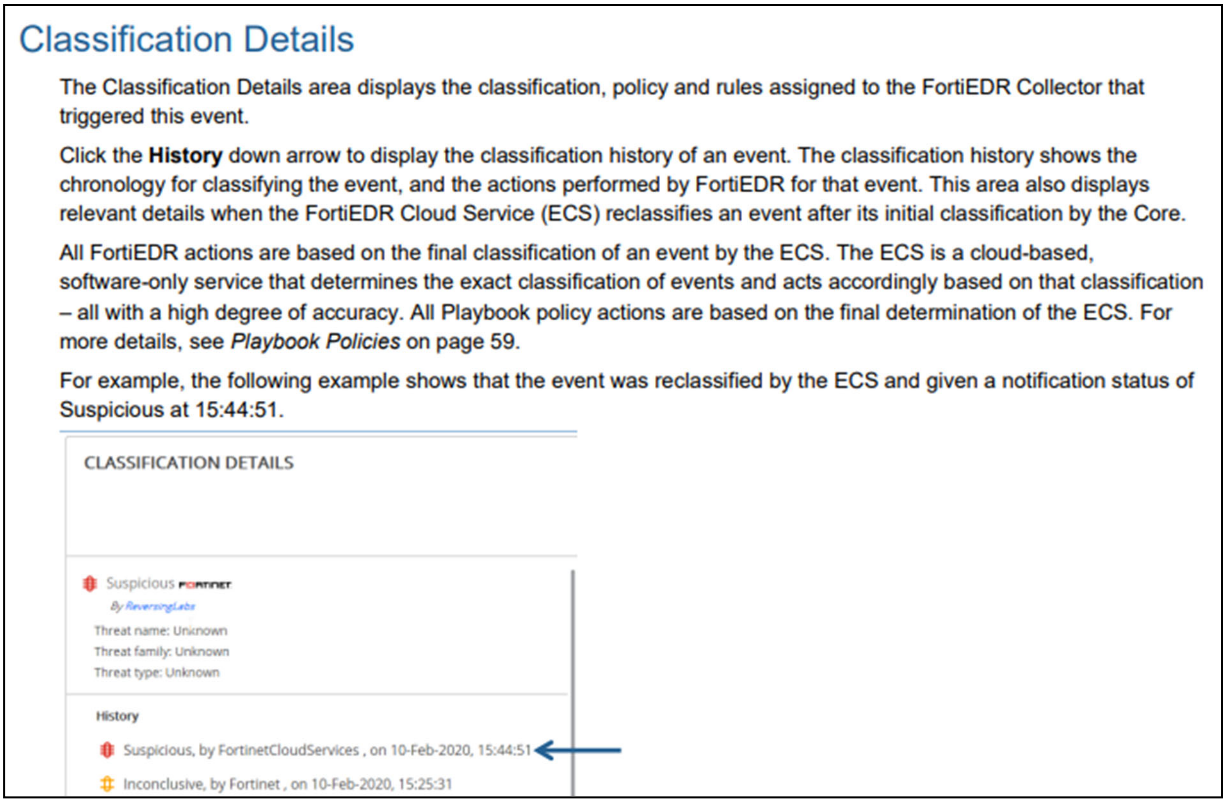
ADVANCED DATA

Event Graph

69

138. Every ’997 Accused Product practices determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store. For example, Fortinet FortiEDR determines a compliance state (e.g., classifies events) of the endpoint based on the status information and the security policies.

[69] https://www.youtube.com/watch?v=_DoSSI9fPAk



Classification Details

The Classification Details area displays the classification, policy and rules assigned to the FortiEDR Collector that triggered this event.

Click the **History** down arrow to display the classification history of an event. The classification history shows the chronology for classifying the event, and the actions performed by FortiEDR for that event. This area also displays relevant details when the FortiEDR Cloud Service (ECS) reclassifies an event after its initial classification by the Core.

All FortiEDR actions are based on the final classification of an event by the ECS. The ECS is a cloud-based, software-only service that determines the exact classification of events and acts accordingly based on that classification – all with a high degree of accuracy. All Playbook policy actions are based on the final determination of the ECS. For more details, see *Playbook Policies* on page 59.

For example, the following example shows that the event was reclassified by the ECS and given a notification status of Suspicious at 15:44:51.

CLASSIFICATION DETAILS

Suspicious FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History
Suspicious, by FortinetCloudServices , on 10-Feb-2020, 15:44:51
Inconclusive, by Fortinet , on 10-Feb-2020, 15:25:31

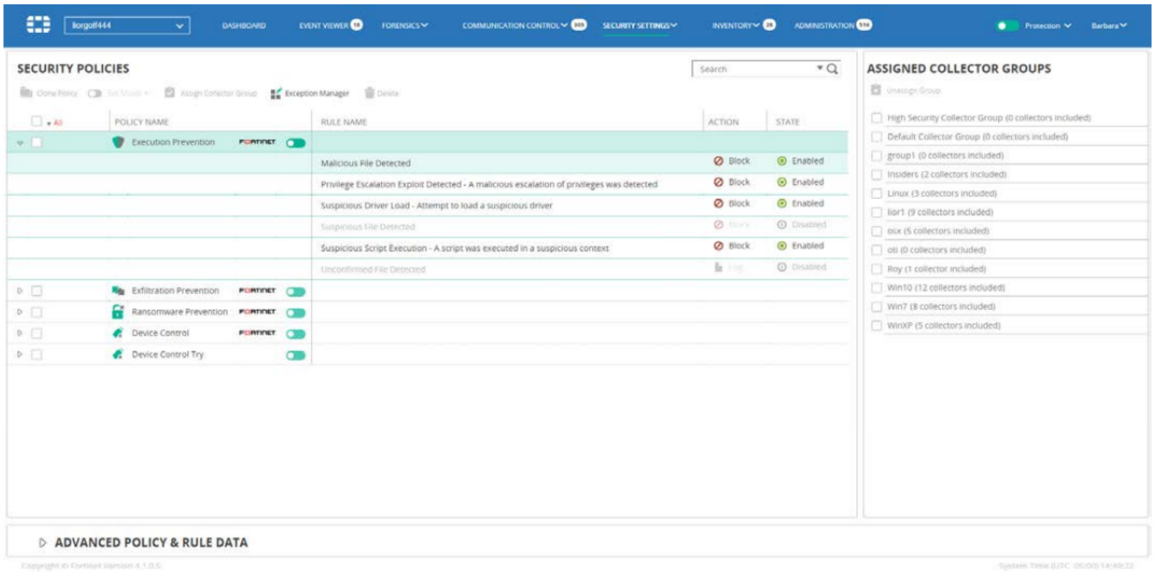
[70]

139. Every ’997 Accused Product practices initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. For example, Fortinet FortiEDR remediation remotely initiates actions identified in the security policies based on the compliance state that are carried out by the endpoint processor.

[70] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf

Security Policies Page

The **SECURITY POLICIES** page displays a row for each security policy. Each policy row can be expanded to show the rules that it contains, as shown below. To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.



POLICY NAME		RULE NAME	ACTION	STATE
Execution Prevention	FORTINET			
		Malicious File Detected	Block	Enabled
		Privilege Escalation Exploit Detected - A malicious escalation of privileges was detected	Block	Enabled
		Suspicious Driver Load - Attempt to load a suspicious driver	Block	Enabled
		Suspicious File Detected	Block	Disabled
		Suspicious Script Execution - A script was executed in a suspicious context	Block	Enabled
		Unconfirmed File Detected	Log	Disabled
Exfiltration Prevention	FORTINET			
Ransomware Prevention	FORTINET			
Device Control	FORTINET			
Device Control Try				

- □ High Security Collector Group (0 collectors included)
- □ Default Collector Group (0 collectors included)
- □ group1 (0 collectors included)
- □ Insiders (2 collectors included)
- □ Linux (3 collectors included)
- □ lior1 (9 collectors included)
- □ osx (5 collectors included)
- □ oti (0 collectors included)
- □ Roy (1 collector included)
- □ Win10 (12 collectors included)
- □ Win7 (8 collectors included)
- □ WinXP (5 collectors included)

FortiEDR is provided out-of-the-box with several predefined security policies (depending on your license), ready for you to get started. By default, all policies are set to **Simulation** mode (meaning that they ***only*** log and ***do not block***) and show the FORTINET logo. This page also enables you to define additional policies.

Exfiltration prevention policies are marked with the icon, ransomware prevention policies are marked with the icon, execution prevention policies are marked with the icon and device control policies are marked with the icon.

The following information is defined per security policy:

Note – Only the **ACTION** (described below) and the **STATE** (Enabled/Disabled) column of a rule can be changed by you.

- **POLICY NAME:** The policy name appears in the leftmost column. The policy name is defined when the policy is created. The name of the **Default Policy** cannot be changed.
- **RULE NAME:** FortiEDR's proprietary rules come predefined and are the primary component of FortiEDR's proprietary security solution. This column displays a short description for the purpose of this rule.

[71]

140. Defendant has and continues to indirectly infringe one or more claims of the '997 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include

[71] *Id.*

infringing technology, such as ’997 Accused Products (*e.g.*, products incorporating the threat classification and remediation features).

141. Defendant, with knowledge that these products, or the use thereof, infringe the ’997 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’997 Patent by providing these products to others, including customers and end-users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, installation manuals, and customer service that instruct end-users to use the products in an infringing manner.[72]

142. Defendant encourages and induces its users and customers of the ’997 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[73]

143. Defendant further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging FortiEDR Collector software to be installed on individual endpoint computers.[74]

144. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability

[72] https://www.fortinet.com/products/endpoint-security/fortiedr/demo;
https://training.fortinet.com/local/staticpage/view.php?page=library_fortiedr; https://training.fortinet.com/;
https://www.fortinet.com/products/endpoint-security/fortiedr;
https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

[73] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[74] https://docs.fortinet.com/document/fortiedr/5.1.0/administration-guide/186029/installing-fortiedr-collectors

that others, including end-users, infringe the ’997 Patent, but while remaining willfully blind to the infringement.

145. Taasera Licensing has suffered damages as a result of Defendant’s direct and indirect infringement of the ’997 Patent in an amount to be proved at trial.

146. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’997 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT VIII
(Infringement of the ’453 Patent)

147. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

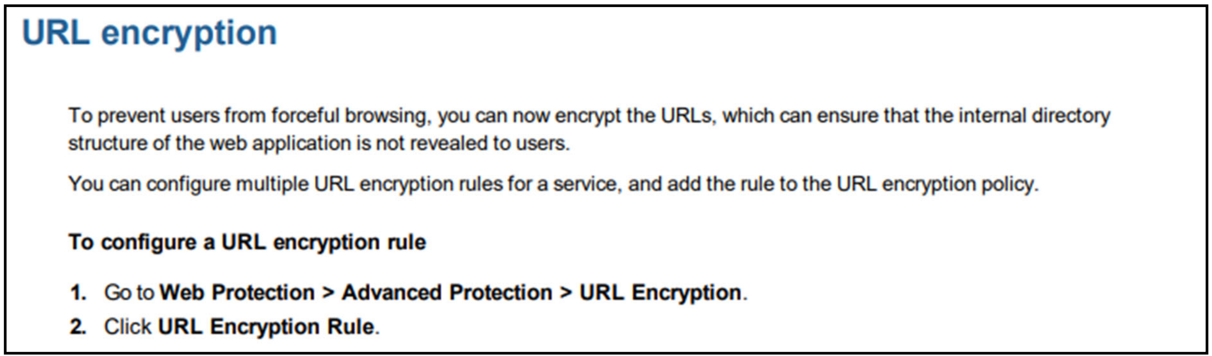
148. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’453 Patent.

149. Defendant has and continues to directly infringe at least claim 13 of the ’453 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’453 Patent. Such products incorporate the URL Encryption feature and include at least Fortinet Fortiweb (the “’453 Accused Products”) which resides on Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’453 Patent.

150. Defendant has and continues to directly infringe the ’453 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’453 Patent. Such products incorporate the URL Encryption feature and include at least Fortinet Fortiweb (the “’453 Accused Products”) which

practices a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; determining, by the computer, whether encryption of the contained URL is required; and determining, by the computer, whether encryption is required for a return URL of the requested resource that is to be returned to a location of the resource request.

151. Every ’453 Accused Product performs restricting access to information transmitted over a computing network. For example, the Fortinet Fortiweb performs URL encryption.



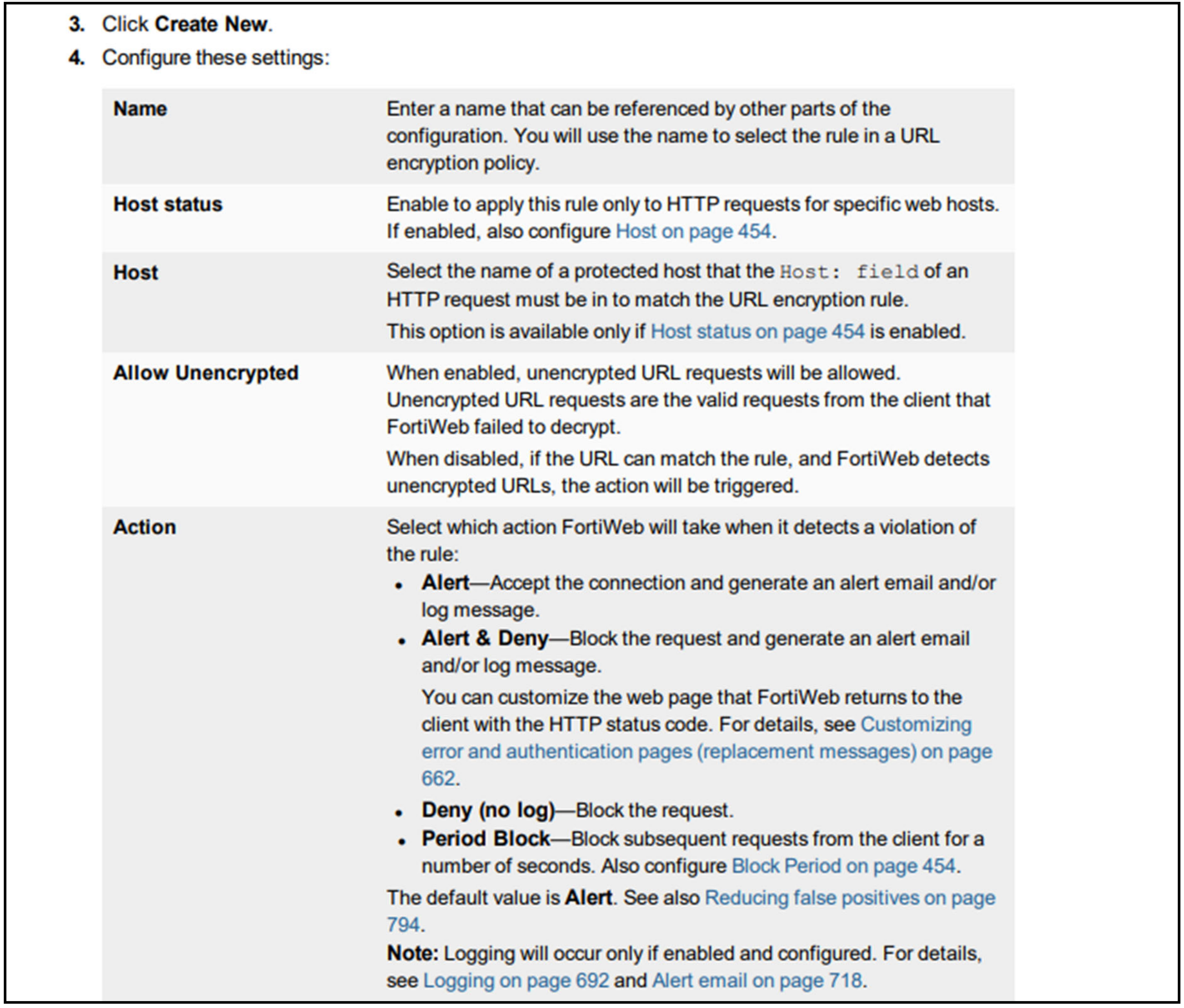
URL encryption

To prevent users from forceful browsing, you can now encrypt the URLs, which can ensure that the internal directory structure of the web application is not revealed to users.

You can configure multiple URL encryption rules for a service, and add the rule to the URL encryption policy.

To configure a URL encryption rule

1. Go to **Web Protection > Advanced Protection > URL Encryption**.
2. Click **URL Encryption Rule**.



3. Click **Create New**.
4. Configure these settings:

Name	Enter a name that can be referenced by other parts of the configuration. You will use the name to select the rule in a URL encryption policy.
Host status	Enable to apply this rule only to HTTP requests for specific web hosts. If enabled, also configure Host on page 454.
Host	Select the name of a protected host that the `Host: field` of an HTTP request must be in to match the URL encryption rule. This option is available only if Host status on page 454 is enabled.
Allow Unencrypted	When enabled, unencrypted URL requests will be allowed. Unencrypted URL requests are the valid requests from the client that FortiWeb failed to decrypt. When disabled, if the URL can match the rule, and FortiWeb detects unencrypted URLs, the action will be triggered.
Action	Select which action FortiWeb will take when it detects a violation of the rule: • **Alert**—Accept the connection and generate an alert email and/or log message. • **Alert & Deny**—Block the request and generate an alert email and/or log message. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see Customizing error and authentication pages (replacement messages) on page 662. • **Deny (no log)**—Block the request. • **Period Block**—Block subsequent requests from the client for a number of seconds. Also configure Block Period on page 454. The default value is **Alert**. See also Reducing false positives on page 794. **Note:** Logging will occur only if enabled and configured. For details, see Logging on page 692 and Alert email on page 718.

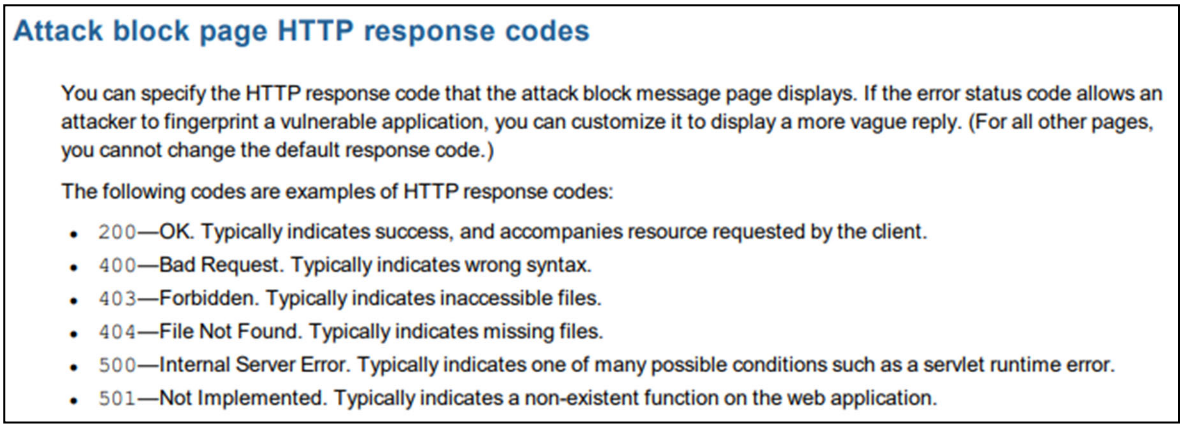
[75]

152. Every '453 Accused Product performs receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a

[75] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/5a6875be-586e-11ea-9384-00505692583a/FortiWeb_6.3.1_Administration_Guide.pdf

universal resource locator (URL). For example, Fortinet Fortiweb receives request URLs for resources to be located.[76]

153. Every ’453 Accused Product performs determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request. For example, if Fortinet Fortiweb is not able to locate the file, it will return a 404 (file not found) error code. Otherwise, the requested resource is available.



Attack block page HTTP response codes

You can specify the HTTP response code that the attack block message page displays. If the error status code allows an attacker to fingerprint a vulnerable application, you can customize it to display a more vague reply. (For all other pages, you cannot change the default response code.)

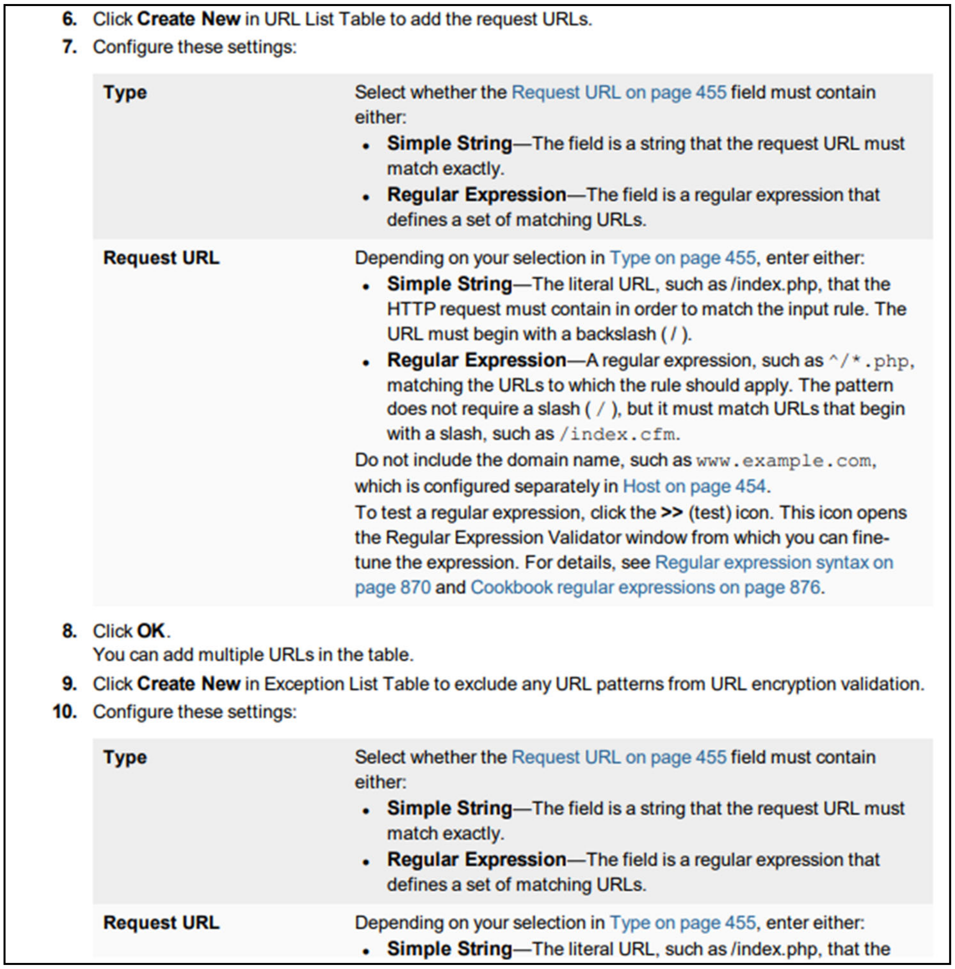
The following codes are examples of HTTP response codes:

- `200`—OK. Typically indicates success, and accompanies resource requested by the client.
- `400`—Bad Request. Typically indicates wrong syntax.
- `403`—Forbidden. Typically indicates inaccessible files.
- `404`—File Not Found. Typically indicates missing files.
- `500`—Internal Server Error. Typically indicates one of many possible conditions such as a servlet runtime error.
- `501`—Not Implemented. Typically indicates a non-existent function on the web application.

[77]

154. Every ’453 Accused Product performs determining, by the computer, whether encryption is required for a return URL of the requested resource that is to be returned to a location of the resource request. For example, Fortinet Fortiweb encrypts all request URLs.

[76] *Id.*
[77] *Id.*



6. Click **Create New** in URL List Table to add the request URLs.
7. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (/). • **Regular Expression**—A regular expression, such as `^/*.php`, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as `/index.cfm`. Do not include the domain name, such as `www.example.com`, which is configured separately in Host on page 454. To test a regular expression, click the **>>** (test) icon. This icon opens the Regular Expression Validator window from which you can fine-tune the expression. For details, see Regular expression syntax on page 870 and Cookbook regular expressions on page 876.

8. Click **OK**.
   You can add multiple URLs in the table.
9. Click **Create New** in Exception List Table to exclude any URL patterns from URL encryption validation.
10. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the

[78]

155. Defendant has and continues to indirectly infringe one or more claims of the ’453 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as ’453 Accused Products (*e.g.*, products incorporating the URL Encryption feature).

156. Defendant, with knowledge that these products, or the use thereof, infringe the ’453 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues

[78] *Id.*

to knowingly and intentionally induce, direct infringement of the ’453 Patent by providing these products to others, including customers and end-users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, deployment guides, and customer service that instruct customers to use the products in an infringing manner.[79]

157. Defendant encourages and induces its users and customers of the ’453 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security products available on its website, widely advertises those products, provides applications that allow customers and users to access those products, provides training and instructions for deploying and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[80]

158. Defendant further encourages and induces its customers to use the infringing Fortiweb product by providing directions for deploying and using Fortiweb.[81]

159. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’453 Patent, but while remaining willfully blind to the infringement.

160. Taasera Licensing has suffered damages as a result of Defendant’s direct and indirect infringement of the ’453 Patent in an amount to be proved at trial.

161. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’453 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

[79] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0

[80] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[81] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0

COUNT IX
(Infringement of the ’251 Patent)

162. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

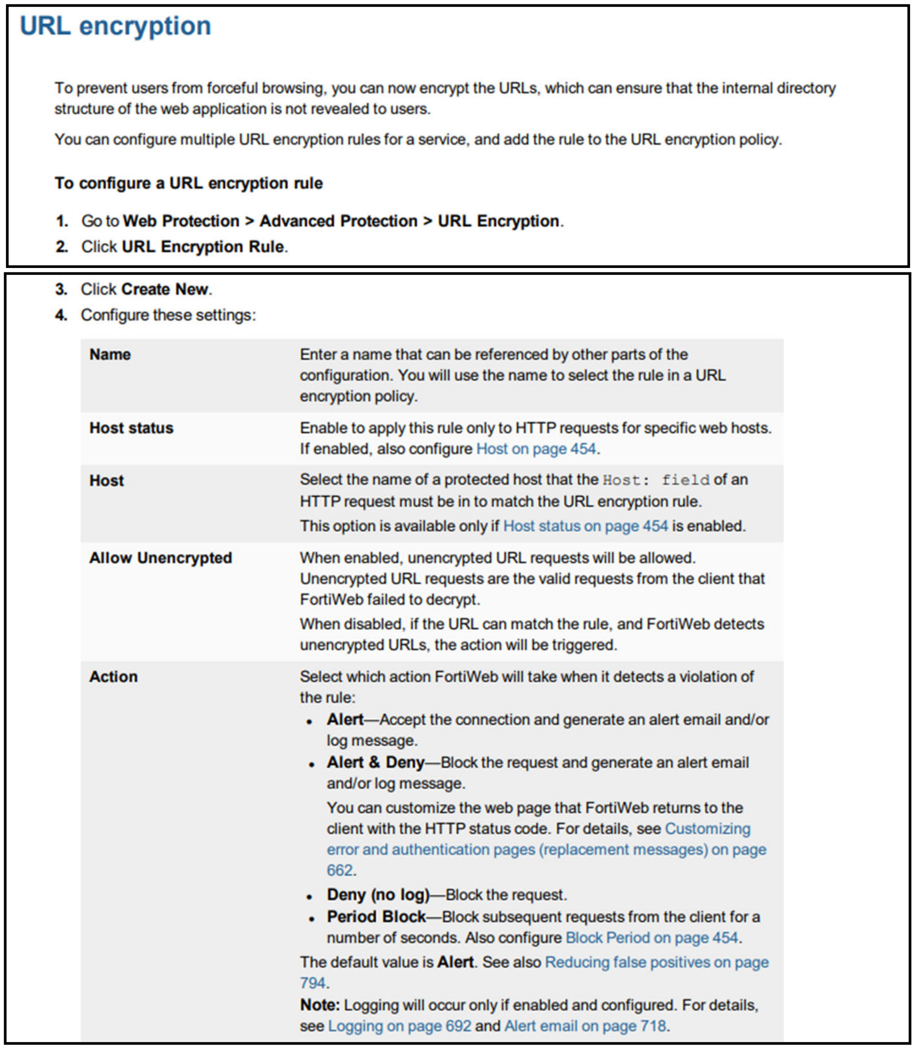
163. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’251 Patent.

164. Defendant has and continues to directly infringe at least claim 7 of the ’251 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’251 Patent. Such products incorporate the URL Encryption feature and include at least Fortinet Fortiweb (the “’251 Accused Products”) which resides on Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’251 Patent.

165. Defendant has and continues to directly infringe the ’251 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’251 Patent. Such products incorporate the URL Encryption feature and include at least Fortinet Fortiweb (the “’251 Accused Products”) is a computer program product, comprising a computer readable hardware storage device containing instructions executable by a computer to implement a method for restricting access to information transmitted over a computing network, said method comprising: receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL); determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request; and after said determining that the requested resource is available, determining,

by the computer, that encryption of the requested resource is required and in response, calculating, by the computer, an encrypted value of the requested resource and sending, by the computer, the encrypted value of the contained URL to the location of the resource request.

166. Every ’251 Accused Product performs restricting access to information transmitted over a computing network. For example, the Fortinet FortiEDR performs URL encryption.



URL encryption

To prevent users from forceful browsing, you can now encrypt the URLs, which can ensure that the internal directory structure of the web application is not revealed to users.

You can configure multiple URL encryption rules for a service, and add the rule to the URL encryption policy.

To configure a URL encryption rule

1. Go to **Web Protection > Advanced Protection > URL Encryption**.
2. Click **URL Encryption Rule**.
3. Click **Create New**.
4. Configure these settings:

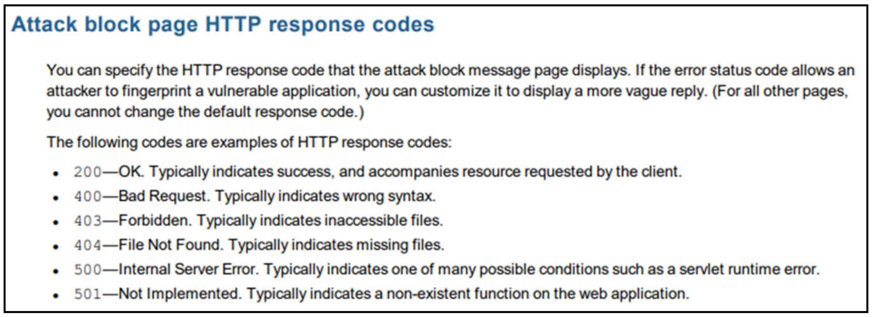
Name	Enter a name that can be referenced by other parts of the configuration. You will use the name to select the rule in a URL encryption policy.
Host status	Enable to apply this rule only to HTTP requests for specific web hosts. If enabled, also configure Host on page 454.
Host	Select the name of a protected host that the `Host: field` of an HTTP request must be in to match the URL encryption rule. This option is available only if Host status on page 454 is enabled.
Allow Unencrypted	When enabled, unencrypted URL requests will be allowed. Unencrypted URL requests are the valid requests from the client that FortiWeb failed to decrypt. When disabled, if the URL can match the rule, and FortiWeb detects unencrypted URLs, the action will be triggered.
Action	Select which action FortiWeb will take when it detects a violation of the rule: • **Alert**—Accept the connection and generate an alert email and/or log message. • **Alert & Deny**—Block the request and generate an alert email and/or log message. You can customize the web page that FortiWeb returns to the client with the HTTP status code. For details, see Customizing error and authentication pages (replacement messages) on page 662. • **Deny (no log)**—Block the request. • **Period Block**—Block subsequent requests from the client for a number of seconds. Also configure Block Period on page 454. The default value is **Alert**. See also Reducing false positives on page 794. **Note:** Logging will occur only if enabled and configured. For details, see Logging on page 692 and Alert email on page 718.

[82]

[82] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/5a6875be-586e-11ea-9384-00505692583a/FortiWeb_6.3.1_Administration_Guide.pdf

167. Every ’251 Accused Product performs receiving, by the computer at a network location, a resource request for a resource to be located, said resource request containing a universal resource locator (URL). For example, Fortinet Fortiweb receives request URLs for resources to be located.[83]

168. Every ’251 Accused Product performs determining by the computer, that the requested resource is available and in response, locating, by the computer, the requested resource contained in the resource request. For example, if Fortinet Fortiweb is not able to locate the file, it will return a 404 (file not found) error code. Otherwise, the requested resource is available.



Attack block page HTTP response codes

You can specify the HTTP response code that the attack block message page displays. If the error status code allows an attacker to fingerprint a vulnerable application, you can customize it to display a more vague reply. (For all other pages, you cannot change the default response code.)

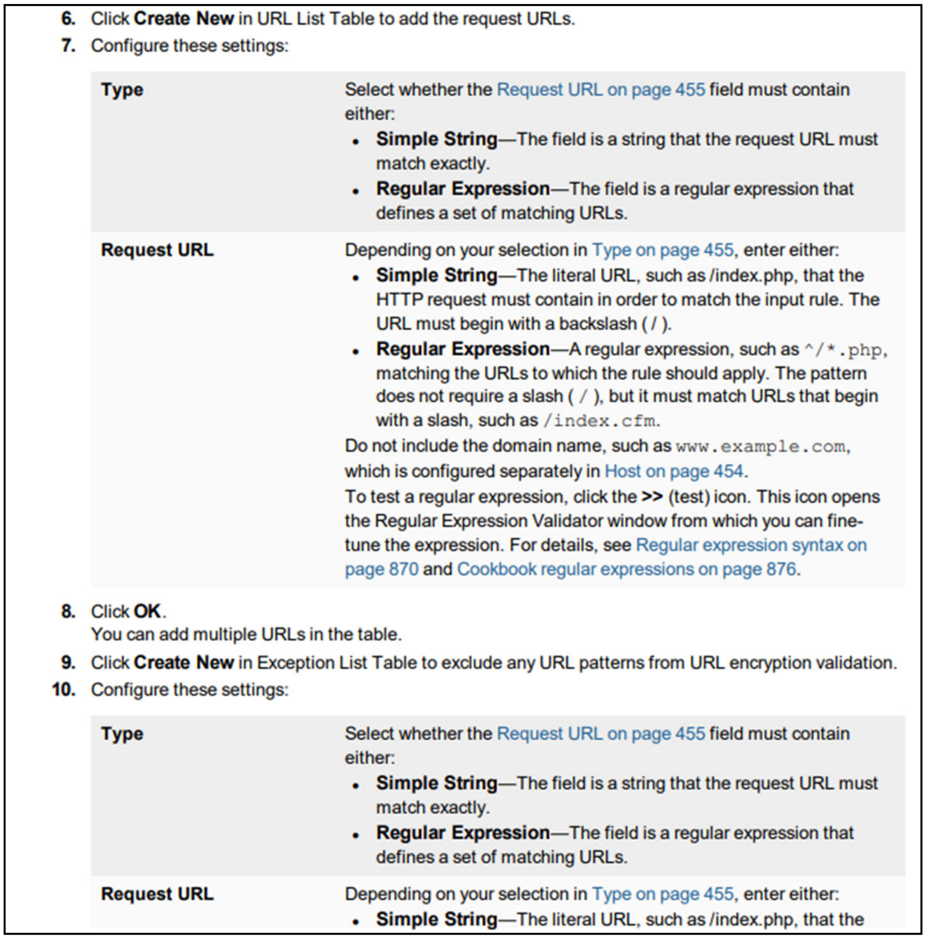
The following codes are examples of HTTP response codes:

- `200`—OK. Typically indicates success, and accompanies resource requested by the client.
- `400`—Bad Request. Typically indicates wrong syntax.
- `403`—Forbidden. Typically indicates inaccessible files.
- `404`—File Not Found. Typically indicates missing files.
- `500`—Internal Server Error. Typically indicates one of many possible conditions such as a servlet runtime error.
- `501`—Not Implemented. Typically indicates a non-existent function on the web application.

[84]

169. Every ’251 Accused Product performs determining, by the computer, that encryption of the requested resource is required and in response, calculating, by the computer, an encrypted value of the requested resource and sending, by the computer, the encrypted value of the contained URL to the location of the resource request. For example, Fortinet Fortiweb encrypts all request URLs and sends the encrypted URL to the location of the resource request.

[83] *Id.*
[84] *Id.*



6. Click **Create New** in URL List Table to add the request URLs.
7. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the HTTP request must contain in order to match the input rule. The URL must begin with a backslash (/). • **Regular Expression**—A regular expression, such as `^/*.php`, matching the URLs to which the rule should apply. The pattern does not require a slash (/), but it must match URLs that begin with a slash, such as `/index.cfm`. Do not include the domain name, such as `www.example.com`, which is configured separately in Host on page 454. To test a regular expression, click the **>>** (test) icon. This icon opens the Regular Expression Validator window from which you can fine-tune the expression. For details, see Regular expression syntax on page 870 and Cookbook regular expressions on page 876.

8. Click **OK**.
   You can add multiple URLs in the table.
9. Click **Create New** in Exception List Table to exclude any URL patterns from URL encryption validation.
10. Configure these settings:

Type	Select whether the Request URL on page 455 field must contain either: • **Simple String**—The field is a string that the request URL must match exactly. • **Regular Expression**—The field is a regular expression that defines a set of matching URLs.
Request URL	Depending on your selection in Type on page 455, enter either: • **Simple String**—The literal URL, such as /index.php, that the

[85]

170. Defendant has and continues to indirectly infringe one or more claims of the ’251 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as ’251 Accused Products (*e.g.*, products incorporating the URL Encryption feature).

171. Defendant, with knowledge that these products, or the use thereof, infringe the ’251 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’251 Patent by providing these

[85] *Id.*

products to others, including customers and end-users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, deployment guides, and customer service that instruct customers to use the products in an infringing manner.[86]

172. Defendant encourages and induces its users and customers of the ’419 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security products available on its website, widely advertises those products, provides applications that allow customers and users to access those products, provides training and instructions for deploying and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[87]

173. Defendant further encourages and induces its customers to use the infringing Fortiweb product by providing directions for deploying and using Fortiweb.[88]

174. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end-users, infringe the ’251 Patent, but while remaining willfully blind to the infringement.

175. Taasera Licensing has suffered damages as a result of Defendant’s direct and indirect infringement of the ’251 Patent in an amount to be proved at trial.

176. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’251 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

[86] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0
[87] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support
[88] https://www.fortinet.com/demo-center/fortiweb-demo; https://docs.fortinet.com/product/fortiweb/7.0

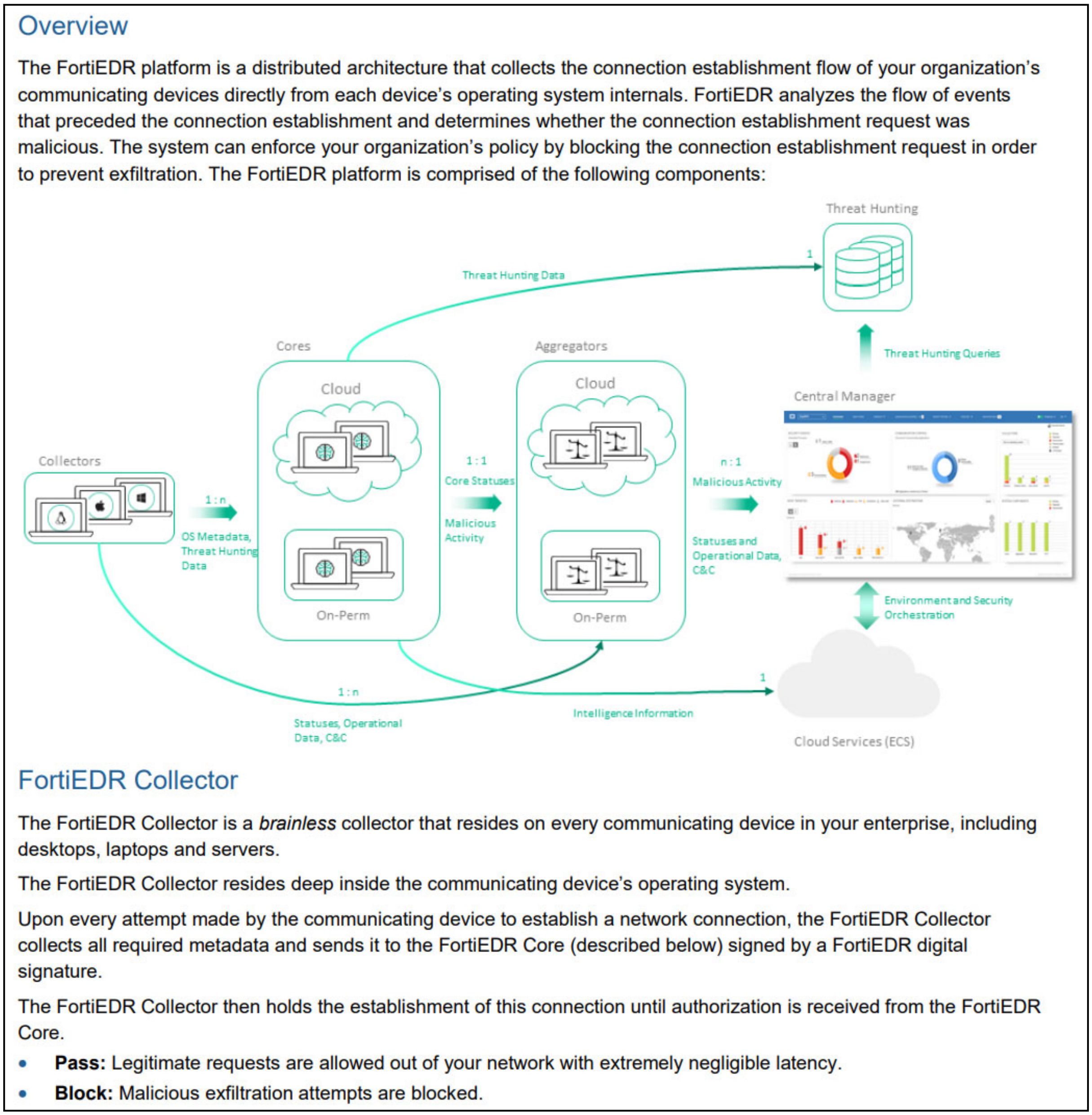
COUNT X
(Infringement of the ’918 Patent)

177. Paragraphs 1 through 36 are incorporated by reference as if fully set forth herein.

178. Defendant is not licensed or otherwise authorized to make, use, offer for sale, sell, or import any products that embody the inventions of the ’918 Patent.

179. Defendant has and continues to directly infringe at least claim 17 of the ’918 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, testing, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’918 Patent. Such products incorporate the behavioral analysis, classification, and authorization features and include at least the Fortinet FortiEDR (the “’918 Accused Products”) which comprise a system for controlling the operation of an endpoint, comprising: a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies; a data store, at the computing system, that contains the plurality of policies; one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies; and one or more hardware processors at the computing system configured to receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, determine, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store, and authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.

180. Every ’918 Accused Product comprises a system for controlling the operation of an endpoint. For example, the Fortinet FortiEDR grants connections on endpoints with authorization from the FortiEDR Core.



Overview

The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization’s communicating devices directly from each device’s operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization’s policy by blocking the connection establishment request in order to prevent exfiltration. The FortiEDR platform is comprised of the following components:

FortiEDR Collector

The FortiEDR Collector is a *brainless* collector that resides on every communicating device in your enterprise, including desktops, laptops and servers.

The FortiEDR Collector resides deep inside the communicating device’s operating system.

Upon every attempt made by the communicating device to establish a network connection, the FortiEDR Collector collects all required metadata and sends it to the FortiEDR Core (described below) signed by a FortiEDR digital signature.

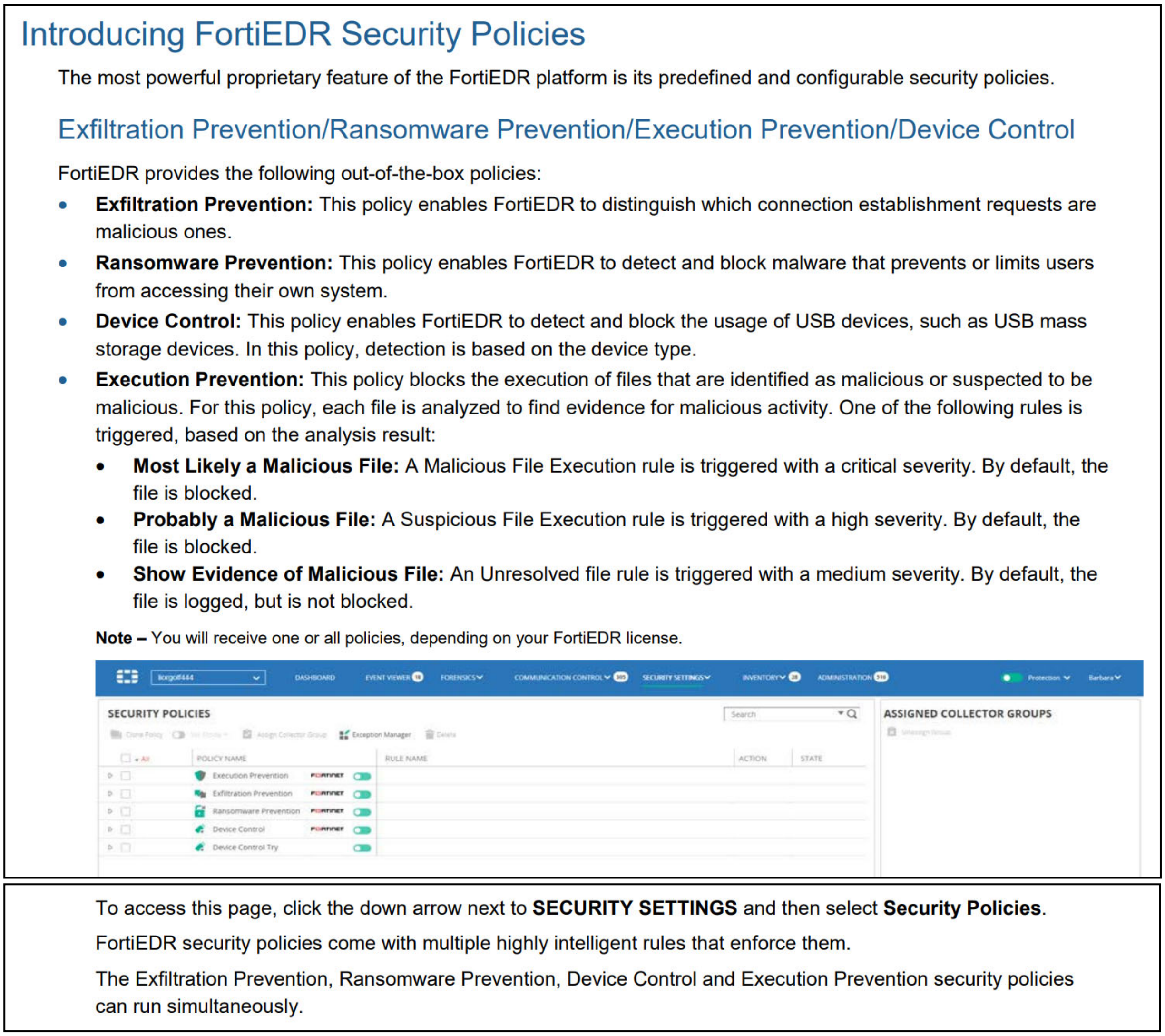
The FortiEDR Collector then holds the establishment of this connection until authorization is received from the FortiEDR Core.

- **Pass:** Legitimate requests are allowed out of your network with extremely negligible latency.
- **Block:** Malicious exfiltration attempts are blocked.

[89]

[89] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

181. Every ’918 Accused Product comprises a user interface, provided by a computing system remote from the endpoint, configured to allow configuration of a plurality of policies, and a data store, at the computing system, that contains the plurality of policies. For example, Fortinet FortiEDR comprises a user interface that allows configuration of a plurality of policies (*e.g.*, security policies) at a system remote from the endpoint which are stored in the FortiEDR data store.



Introducing FortiEDR Security Policies

The most powerful proprietary feature of the FortiEDR platform is its predefined and configurable security policies.

Exfiltration Prevention/Ransomware Prevention/Execution Prevention/Device Control

FortiEDR provides the following out-of-the-box policies:

- **Exfiltration Prevention:** This policy enables FortiEDR to distinguish which connection establishment requests are malicious ones.
- **Ransomware Prevention:** This policy enables FortiEDR to detect and block malware that prevents or limits users from accessing their own system.
- **Device Control:** This policy enables FortiEDR to detect and block the usage of USB devices, such as USB mass storage devices. In this policy, detection is based on the device type.
- **Execution Prevention:** This policy blocks the execution of files that are identified as malicious or suspected to be malicious. For this policy, each file is analyzed to find evidence for malicious activity. One of the following rules is triggered, based on the analysis result:
  - **Most Likely a Malicious File:** A Malicious File Execution rule is triggered with a critical severity. By default, the file is blocked.
  - **Probably a Malicious File:** A Suspicious File Execution rule is triggered with a high severity. By default, the file is blocked.
  - **Show Evidence of Malicious File:** An Unresolved file rule is triggered with a medium severity. By default, the file is logged, but is not blocked.

Note – You will receive one or all policies, depending on your FortiEDR license.

All	POLICY NAME		RULE NAME	ACTION	STATE
▷ □	Execution Prevention	FORTINET			
▷ □	Exfiltration Prevention	FORTINET			
▷ □	Ransomware Prevention	FORTINET			
▷ □	Device Control	FORTINET			
▷ □	Device Control Try				

To access this page, click the down arrow next to **SECURITY SETTINGS** and then select **Security Policies**.

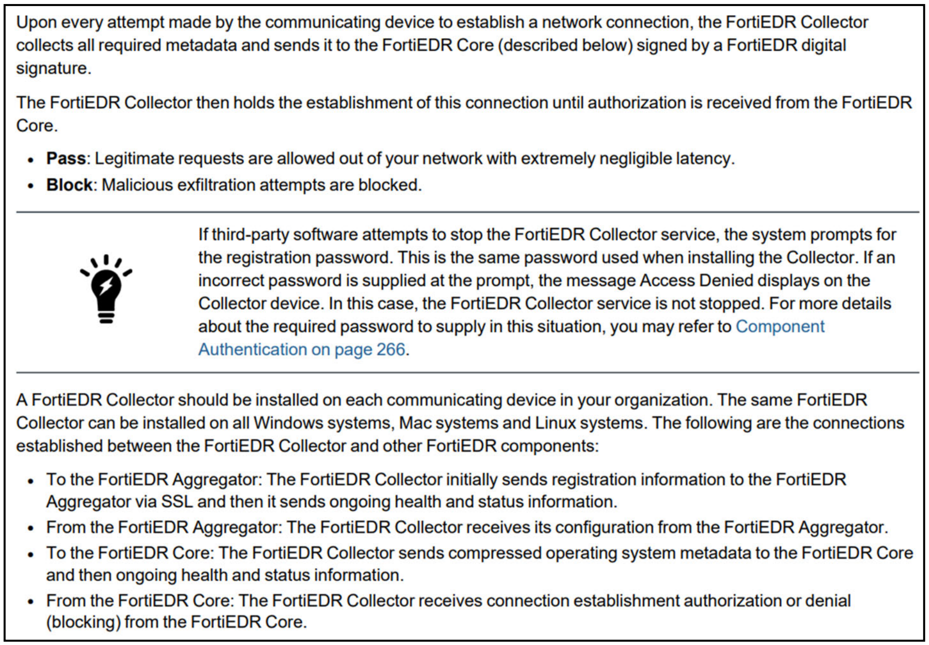
FortiEDR security policies come with multiple highly intelligent rules that enforce them.

The Exfiltration Prevention, Ransomware Prevention, Device Control and Execution Prevention security policies can run simultaneously.

90

[90] *Id*.

182. Every ’918 Accused Product comprises one or more software services, provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies. For example, the Fortinet FortiEDR Collectors evaluate the plurality of operating conditions (*e.g.*, operating system metadata) identified in the security policies.



Upon every attempt made by the communicating device to establish a network connection, the FortiEDR Collector collects all required metadata and sends it to the FortiEDR Core (described below) signed by a FortiEDR digital signature.

The FortiEDR Collector then holds the establishment of this connection until authorization is received from the FortiEDR Core.

- **Pass**: Legitimate requests are allowed out of your network with extremely negligible latency.
- **Block**: Malicious exfiltration attempts are blocked.

If third-party software attempts to stop the FortiEDR Collector service, the system prompts for the registration password. This is the same password used when installing the Collector. If an incorrect password is supplied at the prompt, the message Access Denied displays on the Collector device. In this case, the FortiEDR Collector service is not stopped. For more details about the required password to supply in this situation, you may refer to Component Authentication on page 266.

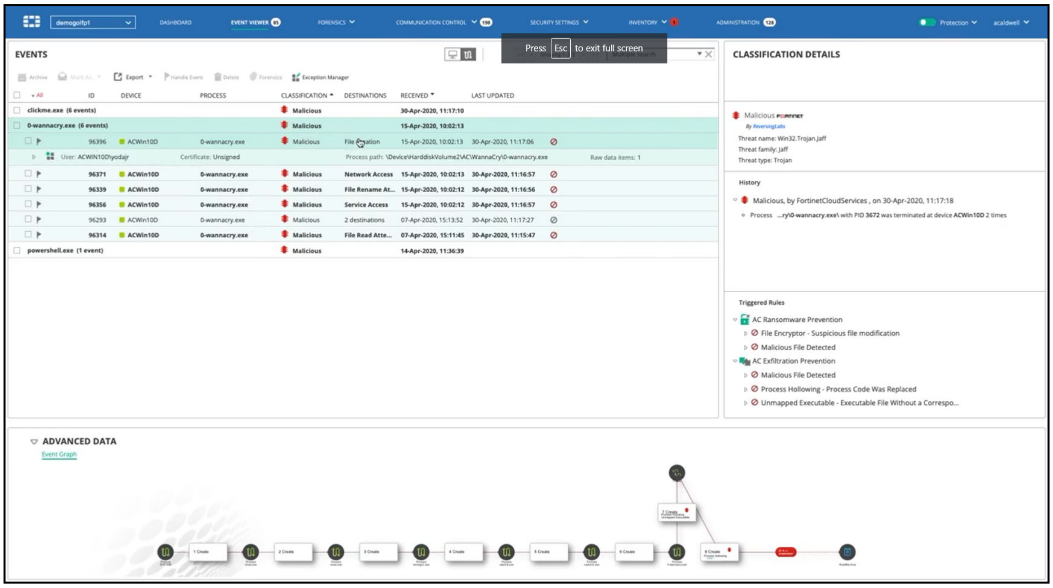
A FortiEDR Collector should be installed on each communicating device in your organization. The same FortiEDR Collector can be installed on all Windows systems, Mac systems and Linux systems. The following are the connections established between the FortiEDR Collector and other FortiEDR components:

- To the FortiEDR Aggregator: The FortiEDR Collector initially sends registration information to the FortiEDR Aggregator via SSL and then it sends ongoing health and status information.
- From the FortiEDR Aggregator: The FortiEDR Collector receives its configuration from the FortiEDR Aggregator.
- To the FortiEDR Core: The FortiEDR Collector sends compressed operating system metadata to the FortiEDR Core and then ongoing health and status information.
- From the FortiEDR Core: The FortiEDR Collector receives connection establishment authorization or denial (blocking) from the FortiEDR Core.

[91]

183. Every ’918 Accused Product receives, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services on the endpoint, and user information that identified a user of the endpoint. For example, FortiEDR receives events, gathered by the one or more software services (*e.g.*, FortiEDR Collectors), and identification of a user of the endpoint.

[91] *Id*.



EVENTS

All	ID	DEVICE	PROCESS	CLASSIFICATION	DESTINATIONS	RECEIVED	LAST UPDATED
clickme.exe (6 events)				Malicious		30-Apr-2020, 11:17:10	
0-wannacry.exe (6 events)				Malicious		15-Apr-2020, 10:02:13	
	96396	ACWin10D	0-wannacry.exe	Malicious	File Creation	15-Apr-2020, 10:02:13	30-Apr-2020, 11:17:06
User: ACWIN10D\yodajr			Certificate: Unsigned		Process path: \Device\HarddiskVolume2\AC\WannaCry\0-wannacry.exe		Raw data items: 1
	96371	ACWin10D	0-wannacry.exe	Malicious	Network Access	15-Apr-2020, 10:02:13	30-Apr-2020, 11:16:57
	96339	ACWin10D	0-wannacry.exe	Malicious	File Rename At...	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:56
	96356	ACWin10D	0-wannacry.exe	Malicious	Service Access	15-Apr-2020, 10:02:12	30-Apr-2020, 11:16:57
	96293	ACWin10D	0-wannacry.exe	Malicious	2 destinations	07-Apr-2020, 15:13:52	30-Apr-2020, 11:17:27
	96314	ACWin10D	0-wannacry.exe	Malicious	File Read Atte...	07-Apr-2020, 15:11:45	30-Apr-2020, 11:15:47
powershell.exe (1 event)				Malicious		14-Apr-2020, 11:36:39	

CLASSIFICATION DETAILS

Malicious FORTINET
By ReversingLabs
Threat name: Win32.Trojan.Jaff
Threat family: Jaff
Threat type: Trojan

History

Malicious, by FortinetCloudServices , on 30-Apr-2020, 11:17:18
- Process ...ry\0-wannacry.exe\ with PID 3672 was terminated at device ACWin10D 2 times

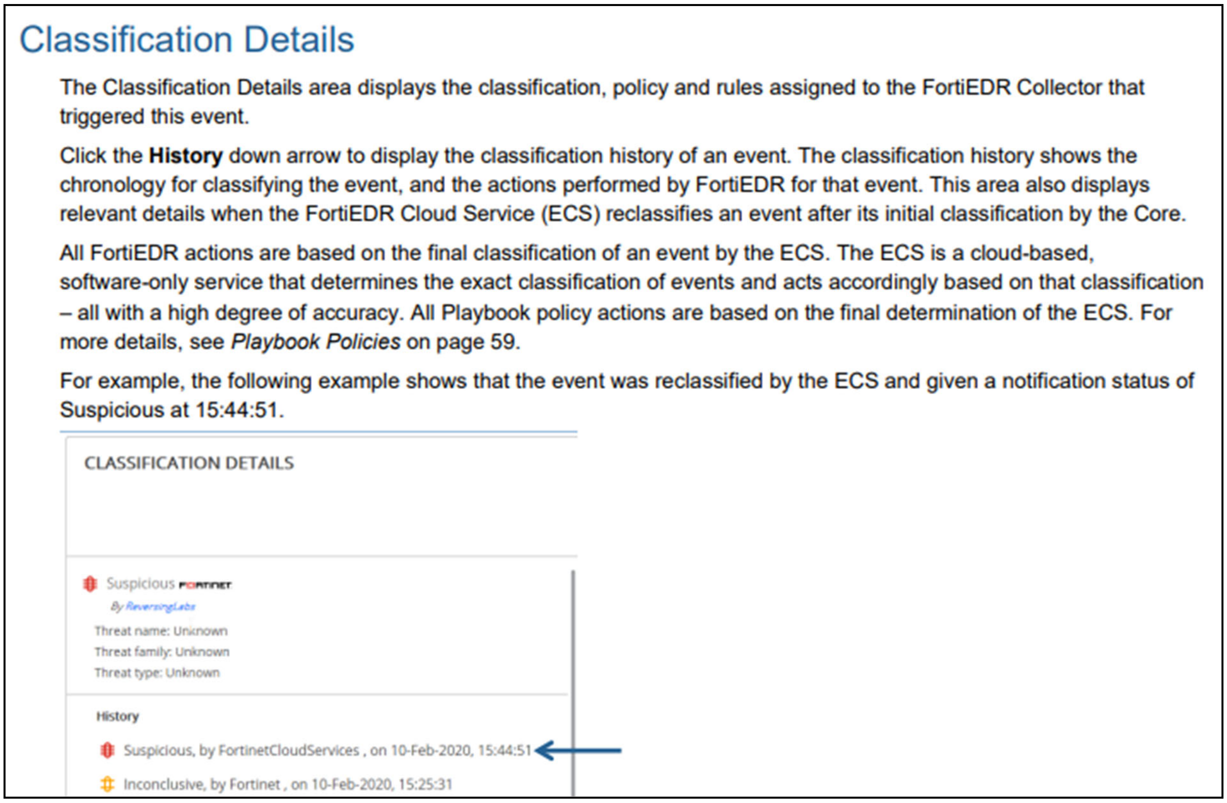
Triggered Rules

- AC Ransomware Prevention
  - File Encryptor - Suspicious file modification
  - Malicious File Detected
- AC Exfiltration Prevention
  - Malicious File Detected
  - Process Hollowing - Process Code Was Replaced
  - Unmapped Executable - Executable File Without a Correspo...

92

184. Every ’918 Accused Product determines, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store. For example, Fortinet FortiEDR determines a compliance state (e.g., classifies events) of the endpoint based on the user information, status information, and the security policies.

[92] https://www.youtube.com/watch?v=_DoSSI9fPAk



Classification Details

The Classification Details area displays the classification, policy and rules assigned to the FortiEDR Collector that triggered this event.

Click the **History** down arrow to display the classification history of an event. The classification history shows the chronology for classifying the event, and the actions performed by FortiEDR for that event. This area also displays relevant details when the FortiEDR Cloud Service (ECS) reclassifies an event after its initial classification by the Core.

All FortiEDR actions are based on the final classification of an event by the ECS. The ECS is a cloud-based, software-only service that determines the exact classification of events and acts accordingly based on that classification – all with a high degree of accuracy. All Playbook policy actions are based on the final determination of the ECS. For more details, see *Playbook Policies* on page 59.

For example, the following example shows that the event was reclassified by the ECS and given a notification status of Suspicious at 15:44:51.

CLASSIFICATION DETAILS

Suspicious FORTINET
By ReversingLabs
Threat name: Unknown
Threat family: Unknown
Threat type: Unknown

History

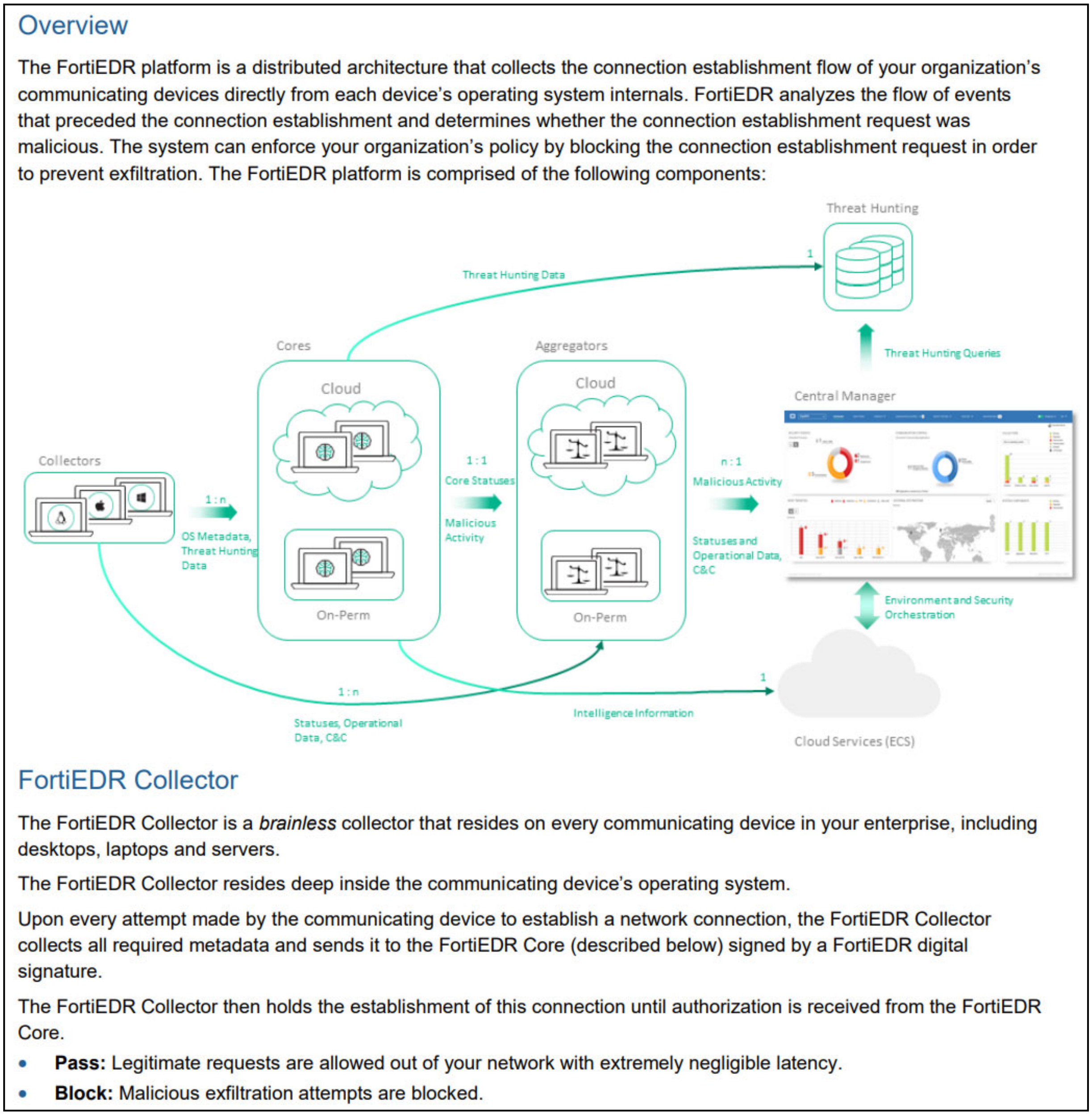
Suspicious, by FortinetCloudServices , on 10-Feb-2020, 15:44:51

Inconclusive, by Fortinet , on 10-Feb-2020, 15:25:31

[93]

185. Every ’918 Accused Product authorizes access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state. For example, the Fortinet FortiEDR Collector authorizes access network connections, authorization being determined by Fortinet FortiEDR in response to the compliance state.

[93] https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9a7241aa-7435-11ea-9384-00505692583a/FortiEDR_Installation_and_Administration_Guide_V4.1.pdf



Overview

The FortiEDR platform is a distributed architecture that collects the connection establishment flow of your organization's communicating devices directly from each device's operating system internals. FortiEDR analyzes the flow of events that preceded the connection establishment and determines whether the connection establishment request was malicious. The system can enforce your organization's policy by blocking the connection establishment request in order to prevent exfiltration. The FortiEDR platform is comprised of the following components:

FortiEDR Collector

The FortiEDR Collector is a *brainless* collector that resides on every communicating device in your enterprise, including desktops, laptops and servers.

The FortiEDR Collector resides deep inside the communicating device's operating system.

Upon every attempt made by the communicating device to establish a network connection, the FortiEDR Collector collects all required metadata and sends it to the FortiEDR Core (described below) signed by a FortiEDR digital signature.

The FortiEDR Collector then holds the establishment of this connection until authorization is received from the FortiEDR Core.

- **Pass:** Legitimate requests are allowed out of your network with extremely negligible latency.
- **Block:** Malicious exfiltration attempts are blocked.

[94]

186. Defendant has and continues to indirectly infringe one or more claims of the '918 Patent by knowingly and intentionally inducing others, including Fortinet subsidiaries, customers, and end-users, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include

[94] *Id.*

infringing technology, such as ’918 Accused Products (*e.g.*, products incorporating the behavioral analysis, classification, and authorization features).

187. Defendant, with knowledge that these products, or the use thereof, infringe the ’918 Patent at least as of the date of this Complaint, knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’918 Patent by providing these products to others, including customers and end-users, for use in an infringing manner, as well as providing demonstrations, training, instruction courses, instruction manuals, installation manuals, and customer service that instruct end-users to use the products in an infringing manner.[95]

188. Defendant encourages and induces its users and customers of the ’918 Accused Products to perform the methods claimed in the Asserted Patents. For example, Fortinet makes its security services available on its website, widely advertises those services, provides applications that allow customers and users to access those services, provides training and instructions for installing, and maintaining those products, and provides technical support to customers and users via the FortiCare support and services.[96]

189. Defendant further encourages and induces its customers to use the infringing Falcon Platform by providing directions for and encouraging FortiEDR Collector software to be installed on individual endpoint computers.[97]

190. Defendant induced infringement by others, including end-users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability

[95] https://www.fortinet.com/products/endpoint-security/fortiedr/demo; https://training.fortinet.com/local/staticpage/view.php?page=library_fortiedr; https://training.fortinet.com/; https://www.fortinet.com/products/endpoint-security/fortiedr; https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/82fbe02c-e479-11eb-97f7-00505692583a/FortiEDR-5.0.0-Installation_and_Administration_Guide.pdf

[96] *Id.*; https://www.fortinet.com/support/support-services/premium-support; https://www.fortinet.com/support

[97] https://docs.fortinet.com/document/fortiedr/5.1.0/administration-guide/186029/installing-fortiedr-collectors

that others, including end-users, infringe the ’918 Patent, but while remaining willfully blind to the infringement.

191. Taasera Licensing has suffered damages as a result of Defendant’s direct and indirect infringement of the ’918 Patent in an amount to be proved at trial.

192. Taasera Licensing has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’918 Patent, for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

DEMAND FOR JURY TRIAL

193. Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Taasera Licensing prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each of the Patents-in-Suit;

b. An order pursuant to 35 U.S.C. § 283 permanently enjoining Defendant, its officers, agents, servants, employees, attorneys, and those persons in active concert or participation with it, from further acts of infringement of the Patents-in-Suit;

c. An order awarding damages sufficient to compensate Taasera Licensing for Defendant’s infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, together with interest and costs;

d. Entry of judgment declaring that this case is exceptional and awarding Taasera Licensing its costs and reasonable attorney fees under 35 U.S.C. § 285; and,

e. Such other and further relief as the Court deems just and proper.

Dated: October 21, 2022

Respectfully submitted,

/s/ Alfred R. Fabricant
Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
Joseph M. Mercadante
NY Bar No. 4784930
Email: jmercadante@fabricantllp.com
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Justin Kurt Truelove
Texas Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston Street
Marshall, Texas 75670
Telephone: (903) 938-8321
Facsimile: (903) 215-8510

ATTORNEYS FOR PLAINTIFF
TAASERA LICENSING LLC